



Management Policy MO Requirements

Candidate Version 1.0 – 14 May 2013

Open Mobile Alliance
OMA-RD-MgmtPolicyMO-V1_0-20130514-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavours to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2013 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

- 1. SCOPE (INFORMATIVE)5
- 2. REFERENCES6
 - 2.1 NORMATIVE REFERENCES.....6
 - 2.2 INFORMATIVE REFERENCES.....6
- 3. TERMINOLOGY AND CONVENTIONS7
 - 3.1 CONVENTIONS.....7
 - 3.2 DEFINITIONS.....7
 - 3.3 ABBREVIATIONS.....7
- 4. INTRODUCTION (INFORMATIVE).....8
 - 4.1 VERSION 1.08
- 5. MANAGEMENT POLICY MO RELEASE DESCRIPTION (INFORMATIVE)9
- 6. REQUIREMENTS (NORMATIVE).....10
 - 6.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS10
 - 6.1.1 Security10
 - 6.1.2 Charging Events.....11
 - 6.1.3 Administration and Configuration11
 - 6.1.4 Interoperability.....11
 - 6.1.5 Privacy11
 - 6.2 OVERALL SYSTEM REQUIREMENTS11
 - 6.2.1 Device Management Server11
 - 6.2.2 Device12
 - 6.2.3 Management Policy12
- APPENDIX A. CHANGE HISTORY (INFORMATIVE).....13
 - A.1 APPROVED VERSION HISTORY13
 - A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY13

Figures

No table of figures entries found.

Tables

- Table 1: High-Level Functional Requirements10
- Table 2: High-Level Functional Requirements – Security Items10
- Table 3: High-Level Functional Requirements – Authentication Items10
- Table 4: High-Level Functional Requirements – Authorization Items.....10
- Table 5: High-Level Functional Requirements – Data Integrity Items11
- Table 6: High-Level Functional Requirements – Confidentiality Items.....11
- Table 7: High-Level Functional Requirements – Charging Events Items11
- Table 8: High-Level Functional Requirements – Administration and Configuration Items11
- Table 9: High-Level Functional Requirements – Interoperability Items11
- Table 10: High-Level Functional Requirements – Privacy Items.....11

Table 11: High-Level System Requirements 11

Table 12: DMS Requirements 12

Table 13: Device Requirements 12

Table 14: Management Policy Requirements..... 12

1. Scope

(Informative)

This document lists the requirement for the OMA DM Management Policy MO Enabler.

2. References

2.1 Normative References

- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997,
[URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)

2.2 Informative References

- [DMDICT] "OMA Device Management Dictionary", Draft Version 1.0 , Open Mobile Alliance™,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMADICT] "Dictionary for OMA Specifications", Version 2.9, Open Mobile Alliance™,
OMA-ORG-Dictionary-V2_9, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Management Policy A rule which describes the Device Management actions to be taken when certain predefined conditions are encountered by the Device.

3.3 Abbreviations

MgmtPolicyMO Management Policy Management Object

4. Introduction

(Informative)

To perform management operations, the DM Server can send the DM commands to the DM Client, and receive the corresponding results from the DM Client. This Request-Response model is the basic characteristics of the DM protocol.

MgmtPolicyMO v1.0 enables a more proactive management approach where the devices are able to perform actions autonomously based on management policies. These policies are pre-defined by the Management Authority and downloaded into the devices via the interface provided by the MgmtPolicyMO. Afterwards the devices will continuously monitor the policies and perform necessary actions. If the policy conditions are met, one or more management actions will be triggered. Possible management actions include, but are not limited to: software management, firmware update, parameter configuration update and initiating a diagnostic and troubleshooting procedure.

After execution, DMS will be notified by the DM Client about the policy management results.

4.1 Version 1.0

MgmtPolicyMO V1.0 covers:

- Download, update, activation, deactivation and removal of management policy(ies) in the device
- Capability to configure specific management policies, composed of conditions and actions, based on MO objects
- Reporting the results of management policy actions to DMS

5. Management Policy MO release description (Informative)

The MgmtPolicyMO Enabler involves the download of management policies to the MgmtPolicyMO Client on the device. The MgmtPolicyMO Client will monitor the specified policy conditions to perform one or more management actions to lead to the desired result (e.g., configuration of the device, resolution of a known problem with an application, etc).

The MgmtPolicyMO V1.0 Enabler is compatible with DM protocol V1.3.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Release
MgmtPolicyMO-HLF-1	The MgmtPolicyMO Enabler SHALL support the download of Management Policy(ies) to the Device.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-2	The MgmtPolicyMO Enabler SHALL support the update of Management Policy(ies) on the Device.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-3	The MgmtPolicyMO Enabler SHALL support the activation/deactivation of Management Policy(ies) on the Device.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-4	The MgmtPolicyMO Enabler SHALL support the removal of Management Policy(ies) from the Device.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-5	The MgmtPolicyMO Enabler SHALL provide a mechanism that allows the Device to indicate the result of MgmtPolicyMO actions to the DM Server.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-6	The MgmtPolicyMO Enabler SHALL support a mechanism to bind related Management Objects so that they can be processed using a single action.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-8	The MgmtPolicyMO Enabler SHALL support the execution of Management Policies, composed of conditions and actions, based on Management Objects.	MgmtPolicyMO 1.0
MgmtPolicyMO-HLF-9	The MgmtPolicyMO Enabler SHALL support the definition of Management Policies, composed of conditions and actions, based on Management Objects.	MgmtPolicyMO 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Release
N/A	N/A	N/A

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

Label	Description	Release
MgmtPolicyMO-ATHEN-1	Only authenticated DM Server SHALL be able to perform MgmtPolicyMO actions on the Device.	MgmtPolicyMO 1.0

Table 3: High-Level Functional Requirements – Authentication Items

6.1.1.2 Authorization

Label	Description	Release
MgmtPolicyMO-ATHOR-1	Only authorized DM Server SHALL be able to perform MgmtPolicyMO actions on the Device.	MgmtPolicyMO 1.0

Table 4: High-Level Functional Requirements – Authorization Items

6.1.1.3 Data Integrity

Label	Description	Release
N/A	N/A	N/A

Table 5: High-Level Functional Requirements – Data Integrity Items**6.1.1.4 Confidentiality**

Label	Description	Release
N/A	N/A	N/A

Table 6: High-Level Functional Requirements – Confidentiality Items**6.1.2 Charging Events**

Label	Description	Release
N/A	N/A	N/A

Table 7: High-Level Functional Requirements – Charging Events Items**6.1.3 Administration and Configuration**

Label	Description	Release
N/A	N/A	N/A

Table 8: High-Level Functional Requirements – Administration and Configuration Items**6.1.4 Interoperability**

Label	Description	Release
MgmtPolicyMO-IOP-01	The MgmtPolicyMO Enabler SHOULD support access to Device system properties provided by MO objects, including date/time, location, Device type and network type.	MgmtPolicyMO 1.0

Table 9: High-Level Functional Requirements – Interoperability Items**6.1.5 Privacy**

Label	Description	Release
N/A	N/A	N/A

Table 10: High-Level Functional Requirements – Privacy Items**6.2 Overall System Requirements**

Label	Description	Release
MgmtPolicyMO-OSR-01	The MgmtPolicyMO Enabler SHALL to use features described in OMA DM v1.3.	MgmtPolicyMO 1.0
MgmtPolicyMO-OSR-02	The MgmtPolicyMO Enabler SHALL support implementation specific extensions.	MgmtPolicyMO 1.0

Table 11: High-Level System Requirements**6.2.1 Device Management Server**

Label	Description	Release
MgmtPolicyMO-DMS-01	The DM Server SHALL be able to query the result of MgmtPolicyMO actions from the Device.	MgmtPolicyMO 1.0
MgmtPolicyMO-DMS-02	The DM Server SHALL be able to receive notifications about the result of MgmtPolicyMO actions from the Device.	MgmtPolicyMO 1.0

Table 12: DMS Requirements**6.2.2 Device**

Label	Description	Release
MgmtPolicyMO-Device-01	The Device SHALL be able to send notifications about the result of MgmtPolicyMO actions to the DM Server.	MgmtPolicyMO 1.0
MgmtPolicyMO-Device-02	The MgmtPolicyMO Enabler SHALL be able to locally invoke DM commands on the various nodes of the Device DM Tree while executing MgmtPolicyMO actions.	MgmtPolicyMO 1.0
MgmtPolicyMO-Device-03	The Device SHALL be able to continuously monitor the Management Policies and trigger actions if conditions are met.	MgmtPolicyMO 1.0

Table 13: Device Requirements**6.2.3 Management Policy**

Label	Description	Release
MgmtPolicyMO-MP-01	The MgmtPolicyMO Enabler SHALL be able to specify a simple condition.	MgmtPolicyMO 1.0
MgmtPolicyMO-MP-02	The MgmtPolicyMO Enabler SHALL be able to specify a simple action.	MgmtPolicyMO 1.0
MgmtPolicyMO-MP-03	The MgmtPolicyMO Enabler SHALL be able to combine simple conditions to define a compound condition.	MgmtPolicyMO 1.0
MgmtPolicyMO-MP-04	The MgmtPolicyMO Enabler SHALL be able to combine simple actions to define a compound action.	MgmtPolicyMO 1.0
MgmtPolicyMO-MP-05	The MgmtPolicyMO Enabler SHALL be able to specify Management Policies in terms of compound conditions and compound actions.	MgmtPolicyMO 1.0

Table 14: Management Policy Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-MgmtPolicyMO-V1_0	09 Jan 2013	All	Baseline document.
	08 Feb 2013	1, 2.2, 3.2, 3.3, 4, 4.1, 5, 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.5, 6.1.6, 6.2	Incorporated CRs: OMA-DM-MgmtPolicyMO-2013-0003R01-CR_Initial_Baseline_Info OMA-DM-MgmtPolicyMO-2013-0004R01-CR_Reqs Editorial changes
	22 Feb 2013	6.1, 6.1.4	Incorporated CRs: OMA-DM-MgmtPolicyMO-2013-0006-CR_EXEC_MamPolicy OMA-DM-MgmtPolicyMO-2013-0007R01-CR_IOP
	23 Apr 2013	4, 5, 6.2.2	Incorporated CRs: OMA-DM-MgmtPolicyMO-2013-0012-CR_Requirement_Clarification OMA-DM-MgmtPolicyMO-2013-0013-CR_RDRR_A003_wording_fix
Candidate Version OMA-RD-MgmtPolicyMO-V1_0	14 May 2013	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2013-0125- INP_MgmtPolicyMO_V1_0_RD_for_Candidate_approval