Device Management Implementation Guide for IoT Solutions

Version 2.3

Stephen Ambrose

6/6/2016

AT&T Internet of Things Solutions Organization
Device Management Guide

Author(s)	Group	Phone #	E-mail
Stephen Ambrose	IoT Solutions	+1 (512) 372-5420	sa2683@att.com
Marvin Fuller	IoT Solutions	+1 (404)713-4761	mf3949@att.com
Steve Hardin	IoT Solutions	+1 (404) 713-2651	sh3153@att.com

AT&T Internet of Things Solutions Organization
Device Management Guide

Abstract

This document is an implementation guide for technical approval of modules and Internet of Things devices (IoT) which focuses on what to consider when implementing OMA-DM or LwM2M for AT&T. Please direct any questions to your IoT Solutions contact.

Revision History

Date	**Revision**	**Description**
7/9/2015	1.6	Withdrew v.16 of ODIS Implementation Guide
7/9/2015	2.0	Initial release of public version of Device Management Implementation guide
8/3/2015	2.1	Added CDR-DVM details for IoT bootstrap accounts.
4/26/2016	2.2	Section 1.5: Added email address for delivery of .csv files. Added requirement for legacy devices manufactured in 2015 & 2016.
6/6/2016	2.3	Section 1.5: Added table showing sample data. Re-added host unique ID into the data set request.

Table of Contents

1. Introduction

AT&T Internet of Things Solutions (IoTS) envisions a scenario where we will enable the ability to provide device management to most of the IoTS devices in our network as a service/solution which may benefit our IoTS partners. This includes all verticals especially all non-computing verticals.

1.1. Device Management Application Types

The types of device management applications that AT&T will deploy will vary according to customer need, but the initial set of device management applications is expected to be from the following:

1) Enablement of device identification and classification via ODIS/DHIR
2) Enablement of firmware upgrade to module via FOTA
3) Enablement of remote configuration of device or radio module
4) Enablement of IoT host device management configuration & command/control
5) Enablement of enhanced security features
6) Enablement of diagnostics data capture and visualization

1.2. Device Management Client Types

Device management (DM) can be implemented with either of two Open Mobile Alliance (OMA) standards. The two standards are OMA-DM or LwM2M (Lightweight Machine to Machine). AT&T IoTS believes that while LwM2M will be the preferred standard for implementing device management on IoTS radio modules and eventually devices, we will allow our partners to choose between an OMA-DM client or LwM2M client for their particular implementations.

1.3. OMA-DM Specifications

The official OMA-DM specifications can be downloaded from the OMA-DM download center at the following link: http://openmobilealliance.org/download-center/

1.4. LwM2M Specifications

The official LwM2M specifications can be downloaded from the LwM2M download center at the following link: http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0

1.5. Feature Support Deadlines and Applicability

Please be aware of the following deadlines for Device Management (DM) functionality as a part of the AT&T certification process:

ODIS/DHIR for New Radio Modules:

- Effective July 1, 2014, **new radio modules** entering the AT&T Network Ready Lab must support OMA-DM ODIS/DHIR.

EXCEPTION: *The radio module will only be utilized by a single model of an integrated device and all TACs used in the radio module will only be utilized for that single integrated device.*

EXCEPTION: *The radio module will only be utilized by computing based devices which by PTCRB rules are required to obtain a unique IMEI TAC per device. (If the module will also be utilized for M2M use cases and does not meet any of the other exception rules then ODIS/DHIR is required).*

FOTA for New Radio Module

- It is desired (optional, not mandatory) that **new radio modules** entering the AT&T Network Ready Lab support FOTA. (The mandatory requirement for all new modules as of April 6th, 2015 has been relaxed.)

New Integrated Devices:

- *(new)* As of April 4, 2016 all **new devices** entering the AT&T Network Ready Lab will be required to support DM ODIS/DHIR or else be assigned a unique TAC on a unique device basis as determined by PTCRB PPMD rules. DM can be implemented with either of two Open Mobile Alliance (OMA) standards, OMA-DM or LwM2M.

  EXCEPTION: *Devices with a unique IMEI TAC assigned for a specific device model name/number (as defined by PTCRB). (Note: In all cases devices are expected to properly increment the IMEI SV field as defined in PTCRB rules.)*
- Manual Alternative: Device OEMs that have not implemented ODIS/DHIR or are using a radio module that does not support ODIS/DHIR by deadlines above can still achieve AT&T certification by providing AT&T with a data file which maps IMEIs to host device information. This data file should be a .csv formatted text file with the following format. One device per line as follows: Host_MFR, Host_SW_Ver, Host_Model, IMEI, Host Device Unique ID. These version numbers are expected to match values corresponding to the AT&T certification. Please note: By choosing this option, the partner must also provide legacy data for all devices manufactured in 2015 and 2016). The data is needed for all carriers, not just AT&T. The data should be provided to AT&T on a recurring 3 monthly basis beginning at the time AT&T TA is granted until ODIS/DHIR is implemented in the device or upon request for an investigation. Email address iotteam@att.com.
- Sample data for the "csv" file is shown in the table below:

HOST_MFR	Host_SW_Ver	Host_Model	IMEI	Host Device Unique ID
ACME Inc	40	Arrow21	357099060399038	99bAEfgXXf
ACME Inc	40	Arrow21	357099060343341	99bAEfgXXf
ACME Inc	40	Arrow21	357099060327658	99bAEfgXXf
ACME Inc	40	Arrow21	357099060347722	99bAEfgXXf
ACME Inc	40	Arrow21	357099060343085	99bAEfgXXf
ACME Inc	40	Arrow21	357099060330397	99bAEfgXXf

1.6. OEM Specific DM Implementations

Some radio module OEMs provide customized or proprietary FOTA or DM solutions to their customers. The requirements in this guide do not prohibit these implementations however all radio modules must still comply with the general ODIS/DHIR/FOTA requirements outlined in this guide. Additional DM accounts as described in Section 1.7 may be used to implement OEM specific solutions.

1.7. DM Account Provisioning

A module will have two factory bootstrap DM Accounts. These will be AT&T default factory DM accounts as defined for IoT modules and devices in 13340 chapter 22. In addition there will be one account that **shall** be left empty at the factory but restricted such that this account can only be programmed in the future by using the NETWPIN method for authentication.. Additional DM Accounts may be provisioned based on OEM requirements.

Account	Usage
1	AT&T Default for IoT modules and devices per Chapter 22 of 13340
2	AT&T Default for IoT modules and devices per Chapter 22 of 13340
3	Blank for OTA bootstrap using NETWPIN method
4+	OEM discretion

The two factory boot strapped DM Accounts will be configured as follows:

<CDR-DVM-3954> First DM Account Parameters - DM 1.2/1.3

Summary: The first DM Account for DM 1.2 will be factory bootstrapped to the lab server per the following table. The use of MD5 or HMAC authentication is mandatory.

DM Account URI	Values
./DMS/Cingular/AppID	w7
./DMS/Cingular/ServerID	ATTLabA
./DMS/Cingular/Name	ATTLabA
./DMS/Cingular/AppAddr/mdm/Addr	https://iotprod.sl.attcompute.com/oma (for secure connection)
/DMS/Cingular/AppAddr/mdm/Port/mdm/PortNbr	Secure connection shall use port 443
./DMS/Cingular/AppAuth/client/AAuthLevel	CLCRED
./DMS/Cingular/AppAuth/client/AAuthType	MD5 or HMAC
./DMS/Cingular/AppAuth/client/AAuthName	Generated using utility in QC defect #25188
./DMS/Cingular/AppAuth/client/AAuthSecret	Generated using utility in QC defect #25188
./DMS/Cingular/AppAuth/client/AAuthData	bnVsbA== (Base 64 encoded value of string “null)
./DMS/Cingular/AppAuth/server/AAuthLevel	SVRCRED
./DMS/Cingular/AppAuth/server/AAuthType	MD5 or HMAC
./DMS/Cingular/AppAuth/server/AAuthName	ATTLabA
./DMS/Cingular/AppAuth/serverAAuthSecret	Generated using utility in QC defect #25188
./DMS/Cingular/AppAuth/serverAAuthData	bnVsbA== (Base 64 encoded value of string “null”)

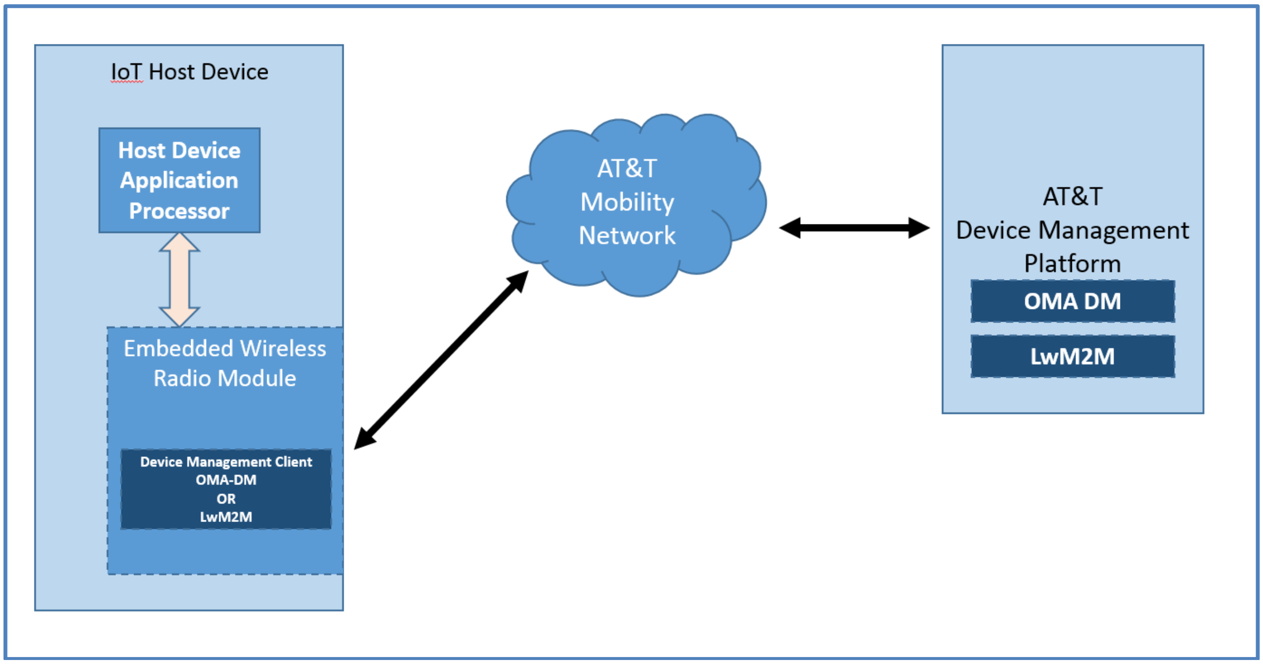
<CDR-DVM-3955> Second DM Account Parameters - DM 1.2/1.3

Summary: The second DM Account for DM 1.2 will be factory bootstrapped to the lab server per the following table. The use of MD5 or HMAC authentication is mandatory.

DM Account URI	Values
./DMS/Cingular/AppID	w7
./DMS/Cingular/ServerID	ATTLabA
./DMS/Cingular/Name	ATTLabA
./DMS/Cingular/AppAddr/mdm/Addr	https://iotdev.sl.attcompute.com/oma (for secure connection)
/DMS/Cingular/AppAddr/mdm/Port/mdm/Port Nbr	Secure connection shall use port 443
./DMS/Cingular/AppAuth/client/AAuthLevel	CLCRED
./DMS/Cingular/AppAuth/client/AAuthType	MD5 or HMAC
./DMS/Cingular/AppAuth/client/AAuthName	Generated using utility in QC defect #25188
./DMS/Cingular/AppAuth/client/AAuthSecret	Generated using utility in QC defect #25188
./DMS/Cingular/AppAuth/client/AAuthData	bnVsbA== (Base 64 encoded value of string “null)
./DMS/Cingular/AppAuth/server/AAuthLevel	SVRCRED
./DMS/Cingular/AppAuth/server/AAuthType	MD5 or HMAC
./DMS/Cingular/AppAuth/server/AAuthName	ATTLabA
./DMS/Cingular/AppAuth/serverAAuthSecret	Generated using utility in QC defect #25188
./DMS/Cingular/AppAuth/serverAAuthData	bnVsbA== (Base 64 encoded value of string “null”)

2. Architecture

To better facilitate an understanding of the Device Management Implementation required by AT&T a diagram is provided below.


IoT Host Device
Host Device Application Processor
Embedded Wireless Radio Module
Device Management Client
OMA-DM
OR
LwM2M
AT&T Mobility Network
AT&T Device Management Platform
OMA DM
LwM2M

2.1. System Components

For the purposes of this implementation Guide, the following components will be referenced:

- Host Device. The IoT Host device could be a wide variety of connected devices usually serving a specific application and could be part of a larger system of connected devices. Examples could include, but are not limited to utility meters, vehicles, asset or fleet tracking devices, security alarm panels, routers or gateways, etc.
- Embedded Wireless Radio Module. The embedded wireless radio module provides wireless connectivity for the Host Device. The embedded wireless radio module has embedded firmware to operate in compliance with the wireless network governing standards, but in most cases will be under the control of the IoT Host Device. For the purposes of this implementation guide, it is assumed that the embedded wireless radio module has an embedded Device Management (DM) Client that could be based on either OMA-DM (Open Mobile Alliance – Device management) or LwM2M (Lightweight Machine to Machine) standards.
- AT&T Mobility Network.
- Device Management Platform. AT&T will manage a DM Platform within our data centers. This platform will be capable of supporting both OMA-DM and LwM2M protocols. The device management platform will be used for various functions including device identification and device firmware upgrades which will be discussed in detail in this document.

2.2. Host Device to Radio Module Interface

When implementing a device management client into the radio module, the module OEM must document and provide an API for the host device OEM to be able to populate the information into the device management client custom nodes inside the radio module. It is at the radio module OEM's discretion to determine how to make the fields available to the host device to populate. (ex. AT Commands, etc.) This interface must be a secure interface which cannot be subject to reverse engineering or monitoring such that the content identifying the host device to AT&T cannot be compromised and potentially utilized to create cloned host devices utilizing a similar IMEI TAC range.

The host device has the responsibility to make sure that the radio module DM client is kept up to date with the correct information at all times. At a minimum, it is recommended that the host device send updated information to the radio module DM client for the following events:

- Host device updates ODIS/DHIR fields in module DM client at initial power up.
- Host device updates ODIS/DHIR fields in module DM client after host device firmware is updated OTA, or locally via USB or other interface.
- Host device updates ODIS/DHIR fields in module DM client after host device detects a system reset to factory defaults. (ex. if these values are not persistent in module through a factory reset procedure)

3. OMA-DM IMEI Sync (ODIS) / Device Host Identity Reporting (DHIR)

3.1. Background

As modules are certified for use on the AT&T network and integrated into various host devices the IMEI TAC range of the module is often leveraged by the integrator of the host device. The PTCRB requirement is that not more than 10,000 units of the host device can use the IMEI TAC range of the embedded module however it has frequently been seen that those rules are not always followed. Whenever a host device leverages the IMEI TAC of the module AT&T has no traceability to the type of host device that the module is installed in and the number of those devices which are present on the network. This lack of traceability is problematic for several reasons including when field issues are discovered with a particular device and we are unable to pin point exactly what those devices are on our network.

To overcome this we have introduced a requirement for all new modules and devices certified on the AT&T network to support a service which reports information to an AT&T database allowing us to identify each discrete device in our network which leverages the IMEI TAC range of the module. This service originally utilized the OMA Device Management (OMA-DM) standard and is known as OMA-DM IMEI Sync (ODIS). This same service is also part of the GSMA Connection Efficiency Guidelines published in 2015 known as Device Host Identity Reporting (DHIR). AT&T has created new custom OMA-DM nodes to collect the information from the host device into which the module is integrated. These requirements were introduced in version 5.4

of 13340 which was released in November of 2013. AT&T will also support the ODIS implementation using Lightweight M2M (LwM2M). This standard is also an OMA developed standard and was introduced to provide a solution for resource constrained devices generally deployed in the Internet of Things domain.

AT&T is making no recommendations as to which OMA-DM or LwM2M client the module manufacturers implement, only that it must support the specified requirements.

3.2. ODIS/DHIR Support Using an LwM2M client

Module implementations are allowed to utilize either LwM2M according to this section or otherwise to implement standard OMA DM. This requirement is applicable to new modules entering the AT&T certification process according to the applicability requirements in section 1.5 of this guideline.

3.2.1. LwM2M Standards Development

At the time of this publication, the LwM2M client does not natively support ODIS/DHIR. AT&T is seeking changes to accommodate ODIS in the Device Object by defining additional resources specifically for the host device. In the interim, AT&T has defined a custom object to be included in modules targeted for certification on the AT&T network. The Object ID for this is Object Id = 16 and is detailed in section 3.2.2 below. Definition of a permanent object and change to the core specification is in progress. Implementation of the permanent object shall be allowed as soon as it is defined and supported by AT&T test capabilities.

3.2.2. LwM2M Object: HostDeviceInfo

Description

This LWM2M Object provides a range of host device related information which can be queried by the LWM2M Server. The host device is any integrated device with an embedded cellular radio module.

Object definition

Name	Object ID	Instances	Mandatory	Object URN
HostDeviceInfo	10241	Multiple	Mandatory	urn:oma:lwm2m:x:10241

Resource definitions

ID	Name	Operations	Instances	Mandatory	Type	Range or Enumeration	Units	Description
5905	Host Device Manufacturer	R	Single	Optional	String			Human readable host device manufacturer name

5906	Host Device Model Number	R	Single	Optional	String			A host device model identifier (manufacturer specified string)
5907	Host Device Unique ID	R	Single	Optional	String			The host device unique ID is assigned by AT&T as the “Device ID” in the onboarding tool and will be stored in
5908	Host Device Software Version	R	Single	Optional	String			Current software version of the host device. (manufacturer specified string).

3.3. ODIS/DHIR Support Using an OMA-DM client

Module implementations of ODIS/DHIR are allowed to utilize either standard OMA DM support according to this section or otherwise implement via LwM2M as defined in section 3.2. This requirement is applicable to new modules entering the AT&T certification process according to the applicability requirements in section 1.5 of this guideline.

3.3.1. Support for OMA-DM Standard Nodes

Standard nodes, as detailed in the OMA specification shall be supported by the module in order to gain visibility to the modules detail and other pertinent Info.

<CDR-DVM-012> OMA Specification Support—OMA Device Management (DM) v1.2 or v1.3
Summary: AT&T requires all devices and modules to support OMA Device Management (DM) v1.2 or v1.3 specifications and mandatory requirements [ERELDDM_1.2] for device provisioning/management.

<CDR-DVM-440> [DMTND]—Device Description Framework Submission
Summary: The vendor shall submit the Device Description Framework (DDF) for the device to AT&T. Device manufacturers shall ensure that the DevDetail, DevInfo and DM Account objects reflect the actual properties and information in use in the device. The DDF is required for LE.

3.3.2. Custom (extension) Node support in the module

Four new custom nodes have been specified to support this effort. Support for these four new custom nodes is mandatory. The nodes must updated as necessary following the update of the device (Host) software version. The following requirement describes the definition of the custom nodes.

Access Type: GET
<CDR-DVM-4532> Support for Module Host Device Reporting in
the Device Detail Management Object
For modules embedded in a host device, the host device
details shall be supported in an extension node within the Device Detail
Management Object. These shall match the PTCRB submission

Host Device Manufacturer

The following OMA-DM node has been defined to specify information related to the manufacturer of the host device, this field will need to match the manufacturer name that is referenced in the AT&T Network Ready Lab certification.

Type: Host Device Manufacturer
Occurrence: One
Format: String
Name: DevDetail/Ext/HostMan
Access Type: GET
The host device manufacturer will be maintained in the node by the
module OMA DM client.

Host Device Model

The following OMA-DM node has been defined to specify the Model name/number of the host device. This must match the model name/number used in the certification of the device.

Type: Host Device Model
Occurrence: One
Format: String
Name: DevDetail/Ext/HostMod
Access Type: GET
The host device model will be maintained in the node by the module OMA DM client.

Host Device Software Version

The following OMA-DM node has been defined to specify the software version of the host device, this information must be populated by the host device manufacturer, must match the version of SW certified by PTCRB and must be updated whenever the SW is updated on the device.

Type: Host Device Software Version

Occurrence: One
Format: String
Name: DevDetail/Ext/HostSwV
Access Type: GET
The host device software version will be maintained in the node by the module OMA DM client

Host Device Unique ID

The following OMA-DM node has been defined to specify the Host Device Unique ID which is equivalent to the AT&T Onboarding Device ID allocated to the host device. The Host Device Unique ID is the ID that is assigned to a device when it is entered into the AT&T onboarding tool through the AT&T Developer portal.

Type: Host Device Unique ID
Occurrence: One
Format: Alphanumeric String
Name: DevDetail/Ext/HostUniqueID
Access Type: GET
The host device unique ID is assigned by AT&T as the “Device ID” in the onboarding tool and will be stored in this node.

Embedded Module IMEI SV

The following OMA-DM node has been defined to enable tracking and verification on the IMEI SV on the embedded module.

Type: IMEI SV
Occurrence: One
Format: Numeric String (2 digit SV)
Name: DevDetail/Ext/IMEISV
Access Type: GET
The IMEI is reported in DevInfo/DevId with the SV to be stored in the IMEI SV node.

4. Firmware Update Over the Air (FOTA)

4.1. Applicability and Client Type

See section 1.5 of this document for applicability. Module OEMs may use either OMA-DM or LwM2M clients for meeting this requirement.

4.2. OMA-DM Firmware Update Management Object (FUMO) Support

OMA-DM clients will use FUMO as the mechanism to perform updates to the module and host device.

4.3. LWM2M Object: Firmware Update

LwM2m clients will use Firmware Update Object (Object ID = 5) as the mechanism to perform updates to the module and host device.

4.4. Proprietary Update

A proprietary solution for updating the module or device FW (either OTA or locally by USB) may also be implemented as long as the following requirement is met.

<CDR-DVM-1533> Device Initiated Session following a non-FOTA Update
Summary: Devices which are updated using one of the following scenarios shall automatically initiate a session with the AT&T Device Management platform to report new device details from the Device Detail Management Object following the update. This is needed to keep AT&T back-end systems in sync with the new device details.

- Device update by sideload/USB
- Device update using a proprietary OEM Device Management server

Note, as well as the standard OMA-DM nodes defined in 13340 it is also required for modules to report the contents of the following custom nodes to the server:

- Host Device Manufacturer
- Host Device Model
- Host Device Software Version
- Host Device Plasma ID

4.5. Memory Allocation in the Module

Module OEMs should make sure that enough memory is included in the design of modules that support firmware updating. There needs to be enough onboard memory to facilitate the updating of the modules itself. Module OEMs should also consider how the client within the module can manage updating of the host device as it relates to memory allocation. It is highly desired that the repository for a pending host device firmware update be stored within the module in a temporary memory but allowance for methods which would require the host device to allocate external memory are also acceptable. Module OEMs will be expected to indicate which method they intend to support for host firmware updates.

5. Device Management Testing

Two phases of testing are defined for the IoTs device management acceptance process. The phases are Interoperability Testing and AT&T Technical Acceptance (TA) testing. All modules must complete Interoperability Testing at an approved lab and submit these results to AT&T prior to commencement of the AT&T TA testing. Host devices using an approved module only need to complete AT&T TA testing and may leverage the Interoperability Testing results from the embedded module.

5.1. Third Party Interoperability Testing

Before any device can be tested against the AT&T Lab or Production instances of the AT&T OMA servers, it must first complete Interoperability Testing against the mFormation platform and the results of this testing must be supplied to AT&T. For information regarding the Interoperability Testing program please refer to AT&T document "17781 ATT Device Management IOT Program Overview". This document can be downloaded from the Digital Asset Management site along with other documents necessary to certify a device on the AT&T network.

5.2. AT&T Technical Acceptance Testing

Specific test cases for each category of module or device can be referenced by filtering 10776 by the columns Test Type = "Device Update."
For each category of device refer to the column labeled "Data Only Module (DOM) "Data and Voice Module (DVM)".

5.3. OMA-DM Test Requirements

Individual and detailed test case descriptions are found in the latest version of AT&T document 15096, Device Update Test Plan.