Document Scope

This application note provides all necessary information to perform Firmware Over-The-Air (FOTA) on Sierra Wireless AirPrime HL Series modules.

This application note applies to AirPrime HL7 and HL8 Series modules implementing OMA LWM2M protocol (e.g. HL8518-S, HL7749, etc).

# FOTA Workflow

The figure below depicts an end-to-end FOTA workflow. It assumes that FW packages (test or final packages) have been made available in AirVantage. This workflow is applicable for validation purposes (prior customer acceptance and deployment) or for field deployment purposes.

The operational process to validate FW packages is not described in this application note.



1. FOTA E2E Workflow

There are 4 main FOTA steps:

1. Register the device in AirVantage, this step has to be applied only once. This registration enables AirVantage to authenticate the module and to perform device management operation. Refer to section Register Device in AirVantage for how to register the device.
2. Discover module’s FW version of your device. Usually, you would need to know the current firmware version before deciding whether a firmware update is needed. This step is performed automatically by the module when connecting to AirVantage for the first time. During this connection, module information (i.e. model, firmware version) is sent to AirVantage. Refer to section Connecting to AirVantage.
3. You can manage FOTA manually using AirVantage web portal (web browser) or programmatically using Web API (out of the scope in this note). Your FOTA operations are persisted until the device connects to AirVantage. Refer to section Create FOTA Operation on AirVantage
4. Manage FOTA operation on the device side. Refer to section Firmware Update OTA

# Register Device in AirVantage

Device must be registered in AirVantage, so that:

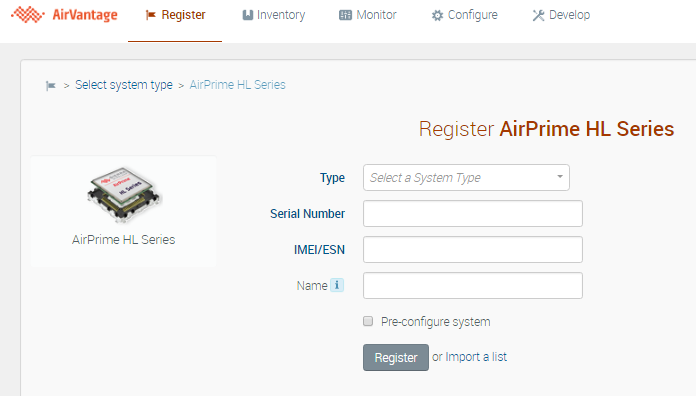
* The device can be authenticated by the server
* The server knows which protocol and what data model to use to communicate with the device

Collect the following information from your embedded module using AT commands:

* Module Type (AT+CGMM)
* Module Serial Number (AT+KGSN=3)
* Module IMEI (AT+CGSN)

To register a device in AirVantage, follow these steps:

1. [Log into Airvantage](https://eu.airvantage.net)
2. If you don’t have an account, sign up for a free trial [here](https://eu.airvantage.net/accounts/signup?type=AVEP).
3. Go to Register page then ‘Select System Type’, as shown in Figure 2 below.
4. Fill in the Type, Serial Number and IMEI/ESN fields with the above information retrieved from the module using AT commands.
5. Provide a Name to your device, this helps to find your system easily
6. Then click on Register to complete the registration procedure



1. AirVantage Web Portal – Registering new System

# Connecting to AirVantage

Device application uses AT commands to make connection to AirVantage and to control FOTA flows.

## Device Management Protocol

AirPrime HL series modules connect to AirVantage DM Server over OMA Lightweight M2M protocol. The DM functions can only be enabled upon successful mutual authentication with AirVantage. If device fails to authenticate with DM server (i.e. due to invalid credentials), it will connect to AirVantage Ligthweight M2M Bootstrap Server to bootstrap the necessary credentials before reattempting to connect to AirVantage DM Server. For further information, please refer to OMA Lightweight M2M protocol specification.

Once a DM session is started, AirVantage can send DM Commands to the device to execute a FOTA (download then install firmware package). The device can also send device information (e.g. fw version, signaling quality) and DM command result back to AirVantage.

The next sections describe how to setup PDP context for this connection and 3 options to trigger a DM session.

### PDP Context

The module uses UDP (CoAP) to communicate with AirVantage in order to create DM sessions.

A DM dedicated PDP context can be assigned for this connection, using the below command:

AT+WDSS=0,”your-apn”,”apn-login”,”apn-password”

To check the current DM dedicated APN setting:

AT+WDSS?

If a DM dedicated APN has not been specified, then CME Error 650 will occur when trying to initiate a connection.

Refer to §8 (APN) for further information on PDP context

### Host Processor Initiated DM Session

To Start DM Session, the host processor (FOTA App) shall issue the following commands

AT+WDSS=1,1

Note :

* only one DM session is open even AT+WDSS=1,1 has been entered multiple times. Subsequent WDSS=1,1 commands do not create new connection but reused the existing connection.
* The session will remain open until the user closes it with AT+WDSS=1,0

Refer to Figure 3, AT Commands Sequence – Host Processor Initiated DM Session.

### Module Initiated DM Session – Polling Mode

The host processor (FOTA Apps) can activate the polling mode on the Module and specifies a polling timer. Upon timer expiration, the module will automatically start a DM session.

The polling timer can be set as follow:

AT+WDSC=3,<pollingDelayMinutes>

Refer to Figure 4, AT Commands Sequence – Device Initiated DM Session, Polling Mode.

## Indications

It is highly recommended to activate Device Services Indications. It enables the host processor application to receive Event Notification asynchronously from the module. The embedded application can selectively subscribe up to 10+ event types. Refer to AT command interface guide for further details.

Enter the following AT command to activate all indications, this shall be done before starting a DM session:

AT+WDSI=8191

To check current indications subscription:

AT+WDSI?

Activating all indications helps the host processor application to keep track of the DM session status and progress. Below is an excerpt indications, refer to AT command guide for full list.

|  |  |
| --- | --- |
| **Indication** | **Event** |
| +WDSI: 0 | SIM is unlocked and APN has been set. Ready for DM session |
| +WDSI: 1 | The device requests an user agreement to connect to AirVantage |
| +WDSI: 2 | AirVantage requests the device to download firmware package |
| +WDSI: 3 | AirVantage requests the device to install the firmware package |
| +WDSI: 4 | The module is starting authentication with AirVantage Bootstrap Server or DM Server |
| +WDSI: 5 | Authentication ended with failure |
| +WDSI: 6 | Authentication succeeded, starting session with the server |
| +WDSI: 23,0 | Session is started with Bootstrap server, i.e. bootstrapping |
| +WDSI: 23,1 | Session is started with DM server, i.e. registering |
| +WDSI: 7 | Connection is denied by server (i.e. Bootstrap server rejects the device, not registered in AirVantage) |
| +WDSI: 8 | DM session has been closed |
| +WDSI: 9 | Firmware package is available for download, also indicates file size |
| +WDSI: 10 | A firmware package has been downloaded and stored in flash |
| +WDSI: 11 | Firmware package has been downloaded but failed to store it into flash |
| +WDSI: 12 | The downloaded package has been verified and is a certified package |
| +WDSI: 13 | The downloaded package is not a certified package |
| +WDSI: 14 | Starting Firmware update |
| +WDSI: 15 | Failed to update firmware |
| +WDSI: 16 | Firmware has been updated successfully |
| +WDSI: 17 | Fallback has been initiated |
| +WDSI: 18 | Download in progress, also indicating the percentage of progress |

The host processor shall not power off the module upon receiving +WDSI:14 and shall wait for the FOTA completion (+WDSI:16) if it needs to do so.

When indication +WDSI: 0 is received, the host processor can start a DM session (AT+WDSS=1,1) anytime. When not receiving it soon after module boot up, the APN shall then be set (WDSS=0,”apn”) and the SIM may need to be unlocked.

## User Agreements

Activating User Agreements enables the host processor application to control the FOTA flow, for instance: the embedded application, busy fulfilling a service (e.g. car is operating, ongoing payment transaction), can decide to postpone firmware download or install operations. As accepting a firmware installation will lead the embedded module to reboot upon FOTA completion.

However, user agreements may be deactivated for other use cases, for instance, the device is not using the module and the device initiates a DM session.

How it works:

If a selected User Agreement has been enabled (WDSC), the module will send a User Agreement Request for the corresponding DM action through Indication (+WDSI), the host processor application shall return a response to this request using WDSR command.

Below is a list of user agreements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **User agreement for a DM action** | **Enable User Agreement** | **Indication Request** | **Agreement Response** | |
| Accept | Defer (can’t refuse) |
| Module requests the user/application to connect to AirVantage | AT+WDSC=0,1 | +WDSI: 1 | AT+WDSR=1  or  AT+WDSS=1,1 | AT+WDSR=0,delay  (delay unit is minute) |
| AirVantage requests the device to download a firmware package | AT+WDSC=1,1 | +WDSI: 2 | AT+WDSR=3 | AT+WDSR=2,delay  (delay > 0) |
| AirVantage requests the device to install the downloaded firmware package | AT+WDSC=2,1 | +WDSI: 3 | AT+WDSR=4 | AT+WDSR=5,delay  (delay > 0) |

If the device is not ready to handle one of the above requested DM action, it is recommended to postpone the request by specifying a delay in number of minutes. Requests can’t be refused. Upon expiration of the delay, the indication will be issued again.

Note that the indication +WDSI:1 is used to request connection to AirVantage upon FOTA completion and module reboot.

The module also supports applicative data exchange functionalities with the server (e.g. AT+AVDATA\* commands), the connection request (+WDSI:1) is not linked to device-orginated or server-orginated data exchanges.

## Connection Flows and AT Commands

Sections §4.1 to §4.2 describe the principle and the corresponding necessary AT commands to start DM session, configure indication and user agreements.

Upon connection trigger (host initiated or module initiated), HL module will attempt to connect to AirVantage DM server :

* Authenticate with DM server, using credentials provided by AirVantage Bootstrap server
* Register with DM Server, in order to send all information about the module to the server, e.g. end point name of the module to be contacted by the server, lifetime, queue mode, LwM2M2 objects and instances within the module.

However, if credentials are missing (very first connection) or invalid (i.e. 3 consecutive failures to authenticate with DM server) then HM module will automatically connect to AirVantage Bootstrap server:

* Authenticate with Bootstrap server (bootstrap server credentials have been provisioned by Sierra Wireless in factory)
* Start bootstrapping credentials : the module issue a Bootstrap request, the bootstrap server writes credentials (to connect to DM server) onto module LwM2M server objects

Note that the module may delete the DM credentials upon 3 consecutives Registration failure, this will force the module to reconnect to the bootstrap server to update credentials.

To increase the security, AirVantage implements key rotation, this forces the module to connect to bootstrap server on a regular basis to receive new credentials, upon authentication failure :

* DM Server invalidates the device credentials every 90 days. The device will fail to authenticate to DM server forcing it to connect to the bootstrap server to update the credentials.
* The bootstrap server is also performing device credentials rotation on a random basis : between 30 to 45 days interval.

+WDSI:23,1 indicates that module is connected to AirVantage DM server. This connection remains opened until the host explicitely closes it with AT+WDSS=1,0

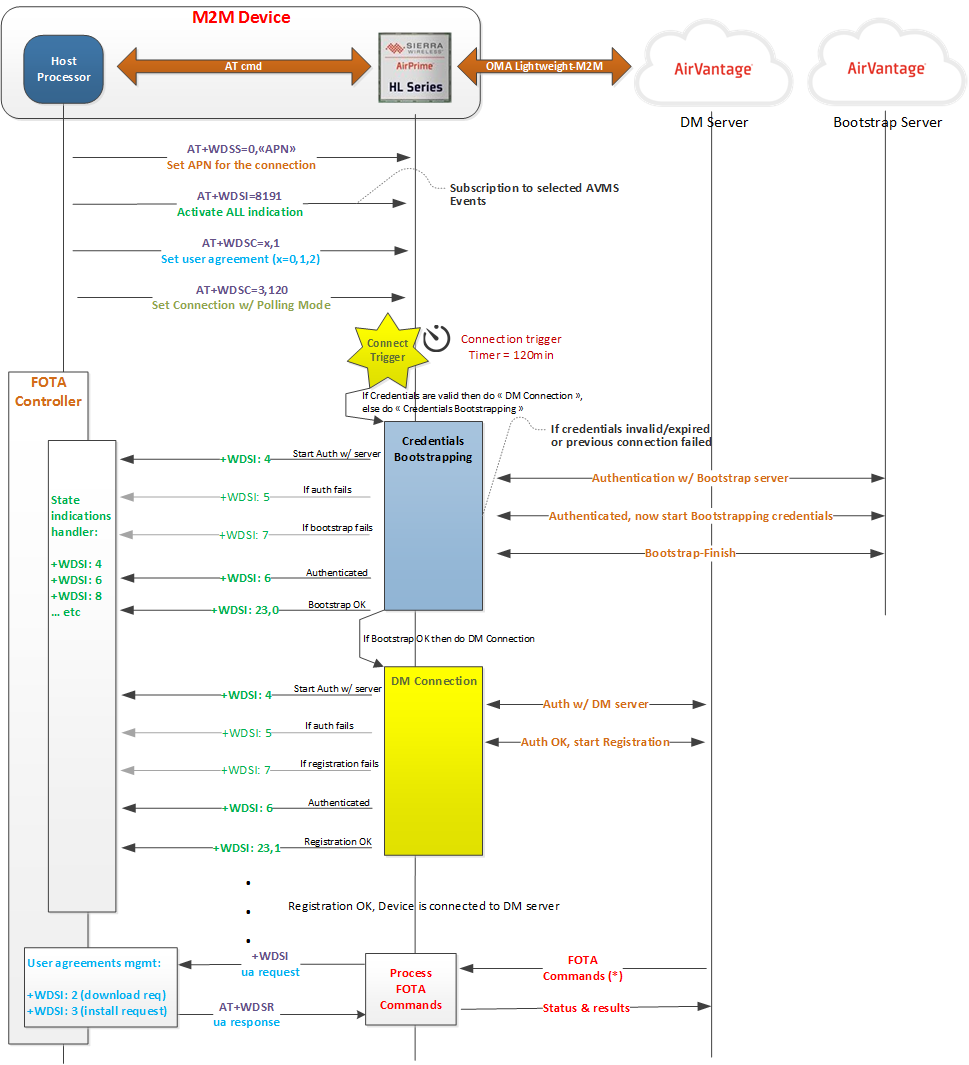
Figures below depict the usage of these AT commands in a proper sequence, for each type of DM session trigger use case.

### Host Processor Initiated DM Session

### 

1. AT Commands Sequence – Host Processor Initiated DM Session

### Device Initiated DM Session – Polling Mode



1. AT Commands Sequence – Device Initiated DM Session, Polling Mode

In this example, the polling timer is set to 120 minutes, the module will be connecting to AirVantage DM server every 2 hours. The connection is not automatically closed.

### Restore Downstream Communication

When the device opens a DM session (§4.4.1 or §4.4.2), AirVantage keeps track on device’s IP address and port number, so that DM operations (FOTA, Synchronize etc) set by user can be sent immediately to the device.

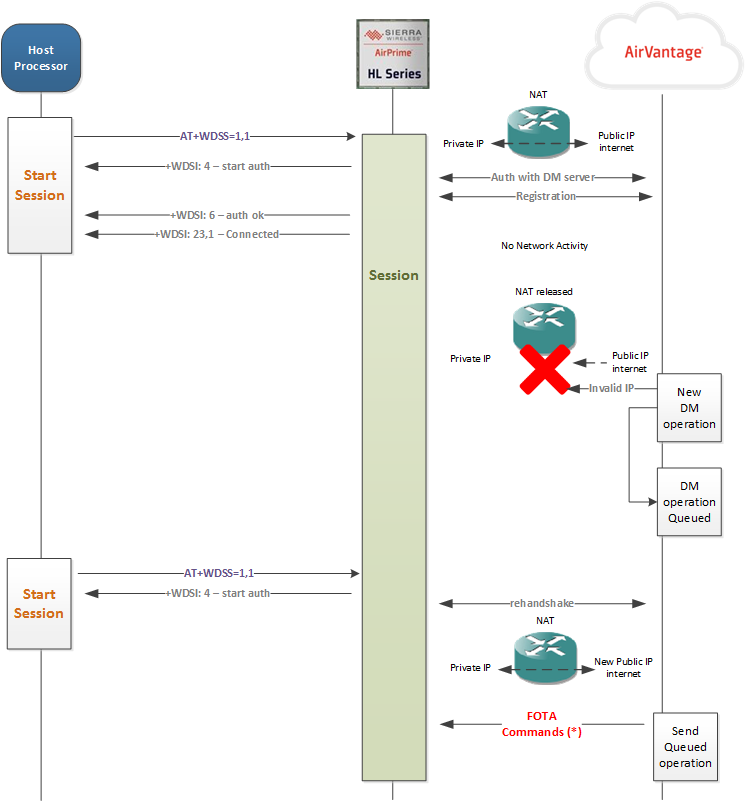
In some situations, user’s DM operations cannot be sent ot the device and are queued in AirVantage:

* DM session is not open
* DM session has been started but the network operator has release the NAT after a short period of inactivity on the network.

The term “session” used above is related to a DM session (from LWM2M Register to Unregister). A DM session remains open until the user closes it (refer to §4.1.2). LWM2M protocol is based on UDP which is not a connection oriented protocol. If there is no network activity, the operator network may release the NAT to yield the resource to other users. When the NAT is released, the device’s external IP address and port number are no longer valid, the downstream communication is broken and AirVantage cannot send user DM operation to device. However the DM session is still active as the device can still send data to AirVantage.

To restore the downstream communication, the device can :

* send data to AirVantage (AT+AVDATA\* commands, not covered in this note)
* send a Registration Update message to AirVantage, by issuing AT+WDSS=1,1. As the session is already open, this command will not open a new session but rather perform a rehandshaking with the server.



1. Network operator NAT release – Restoring downstream communication

## Testing

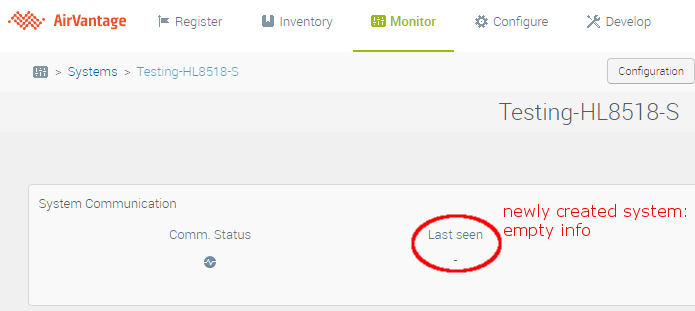
The following tests verify the connectivity of DM session.

### Create New System in AirVantage

Following the section Register Device in AirVantage, a new system (labeled Testing\_HL8518-S) is created in AirVantage.

Go to Monitor/Systems or Upgrade/Systems (if UFOTA account) view then select the newly created system.

In the “System Communication” widget, the “Last seen” field is empty as the new system has never connected to AirVantage. See below screen capture.



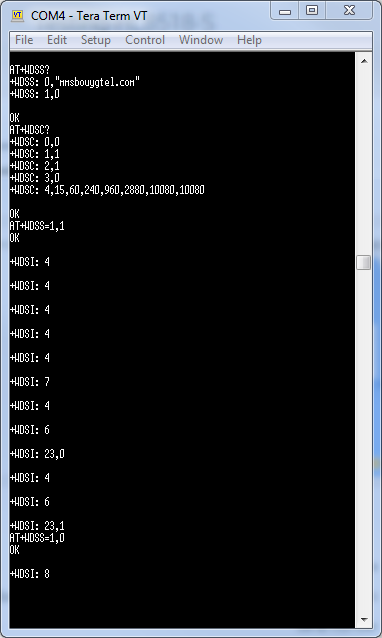
### Connect the Module to AirVantage

Refer to section §4.4.1 Host Processor Initiated DM Session to trigger a DM session:

* Set the APN
* Check APN (AT+WDSS?)
* Activate 2 user agreements (AT+WDSC=1,1 & AT+WDSC=2,1)
* Check user agreements setting (AT+WDSC?)
* Initiate a DM session (WDSS=1,1)

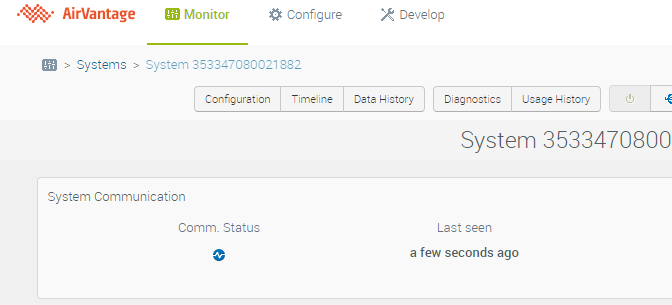
In this example, the module attempts to connect with the DM server with several retries, upon failure it connects to bootstrap server to update the credentials (+WDSI:23,0), then successfully connected to DM server (+WDSI:23,1)

Note the connection remains opened until we explicitely close it with AT+WDSS=1,0. +WDSI:8 indicates the connection is closed.

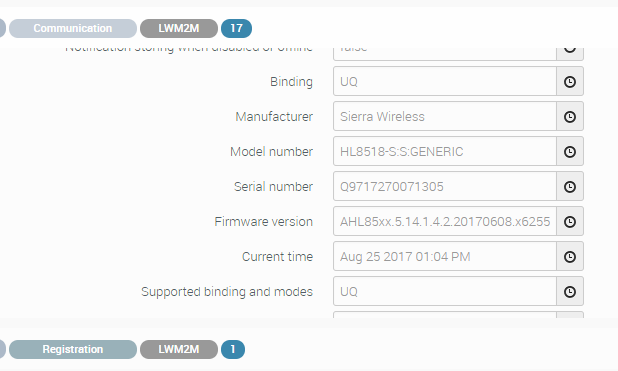


### View Device Data in AirVantage

Return to AirVantage portal and refresh the page, we now see the “Last seen” field indicates a connection from the module.



Data sent by the module to AirVantage can be visualized in the “Timeline” widget: Current firmware version, model, etc…

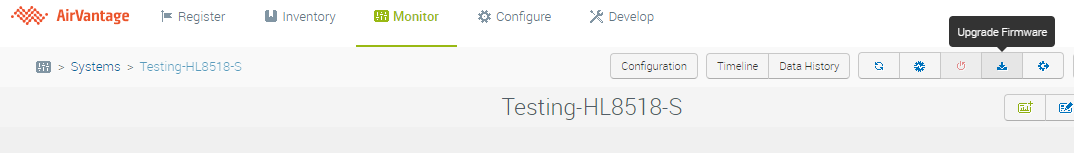


Note that the current firmware version of the module is sent to DM server.

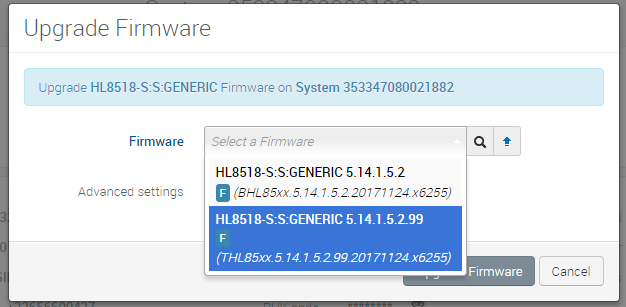
# Create FOTA Operation on AirVantage

Proceed as follow to create a FOTA operation on AirVantage:

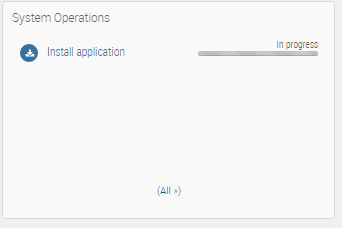
1. [Log into Airvantage](https://eu.airvantage.net)
2. If you don’t have an account, sign up for a free trial [here](https://eu.airvantage.net/accounts/signup?type=AVEP).
3. Go to Monitor/Systems or Upgrade/Systems (if UFOTA account) view and select your device
4. Note the current firmware version of your device in the “System Info” widget. This information shall have been updated during the last DM session (for your reference, refer to section Testing)
5. Click on the “Update firmware” button, as depicted below



1. Select the target firmware version for the FOTA operation. Note only compatible packages are listed.



1. The FOTA operation, also referenced generically as “Install Application”, shall now be “in progress” state



# Firmware Update OTA

When a FOTA operation is created on AirVantage (refer to section5, Create FOTA Operation on AirVantage), the module will start the firmware download and installation procedure as soon as it opens a DM session (refer to section4) with AirVantage.

Download request (+WDSI:2) and Installation request (+WDSI:3) indications are used to catch the events. User agreement AT commands (AT+WDSR) are then used to accept/delay/reject the request. Refer to section User Agreements.

This section describes 2 FOTA use cases: with and without User Agreements.

## No User Agreement

User agreements are activated by default. It is recommended leave them activated, however it may be bypassed when the host processor initiates DM session (section §4.4.1) during specific cycle (e.g. shutting down system, check for firmware upgrade before powering the device off, etc)

The DM session initiation is the same as section §4.4.1, but the user agreements are deactivated.

Refer to Figure 6, No User Agreement FOTA – Host processor Initiated DM Session.

For simplicity, this depicted flow assumes that the credentials are valid, thus connection to bootstrap server is not required.

Please note that indications +WDSI:12 and +WDSI:14 are fired before +WDSI:6 and +WDSI:23,1 have a chance to do so, this may be confusing, but per LwM2M specification, DM server can only issue DM and enablement services commands only after device registration success (+WDSI:23,1). Therefore host’s FOTA controller should not implement the FOTA logic based on the ordering of indications.

## User Agreement

Even though the device is busy fulfilling services, it can decide on the action to be taken when FOTA request arises. User Agreement commands (section §4.3) allows the host processor to accept/delay/reject the FOTA request (download & install).

Figure 7, FOTA flow controlled by user agreement, depicts the sequence for a FOTA operation triggered by wake-up SMS sent from AirVantage.

For simplicity, this depicted flow assumes that the credentials are valid, thus connection to bootstrap server is not required.

Please note that indication +WDSI:3 might be returned before +WDSI:6 and +WDSI:23,1 have a chance to do so, this may be confusing, but per LwM2M specification, DM server can only issue DM and enablement services commands only after device registration success (+WDSI:23,1). Therefore host’s FOTA controller should not implement the FOTA logic based on the ordering of indications.

A request can be postponed by specifying a delay period in minute. Upon expiration of the delay, the module will send the same request again. It can be postponed again or accepted. Refer excerpt in Figure 8, Delaying a Request.

When user agreement is required for package download and install, the module keeps waiting for a response (AT+WDSR). If there is no response, then the same user agreement request (+WDSI) will be send again every 30 minutes.

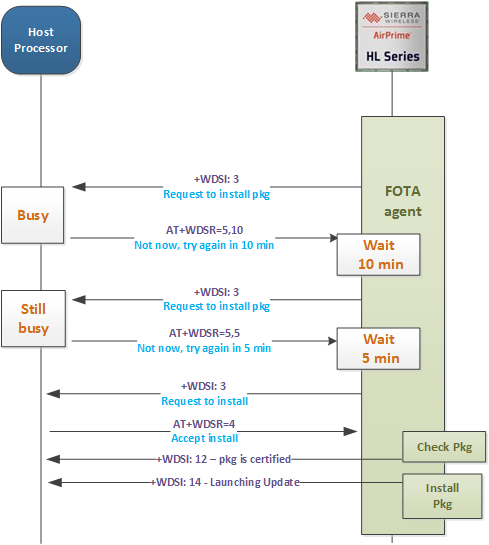
When the user agreement for connection is enabled, the module will send a request to host processor asking for connection to server. In this event, the host processor application can trigger a connection (AT+WDSS=1,1) immediately or later.



1. No User Agreement FOTA – Host processor Initiated DM Session



1. FOTA flow controlled by user agreement



1. Delaying a Request

## Firmware Package Security

Firmware packages are signed with a private key. Before starting the firmware installation, the module checks the validity of the download package. This verification makes use of an embedded RSA 2048-bits public key.

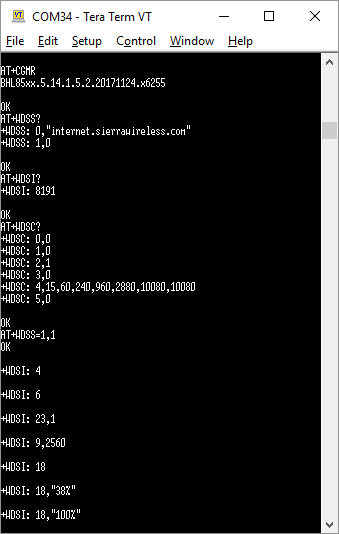
## Update and Timing

Upon receiving +WDSI:14, which indicates the beginning of the Firmware Update, your application shall not power off the module and shall wait for the end of this process: +WDSI:15 (failure) or +WDSI:16 (success). Firmware update duration depends on the type of the package (delta package or full package), the package size and the complexity of the difference between 2 images (delta package). For the latter case, the image difference could be mainly incremental or differential. In general, the update duration ranges from 1 to 8 minutes. Should you need to setup a watchdog, a timer of 15 minutes should provide a safe margin.

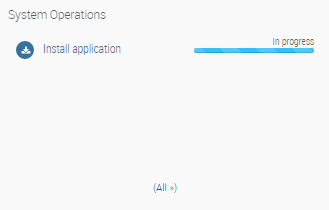
## Testing

In the previous section Create FOTA Operation on AirVantage, a FOTA operation has been created on AirVantage. To trigger it on the device side:

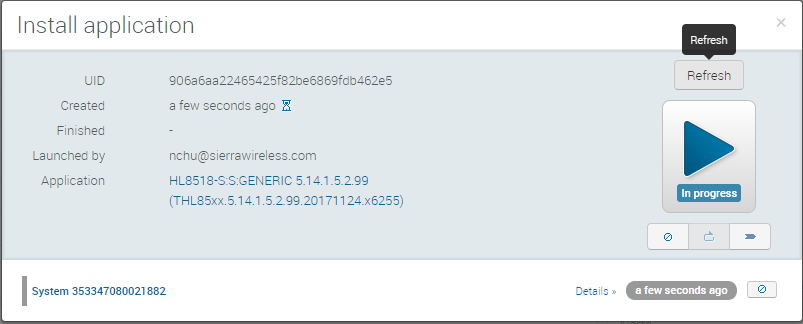
* AT+CGMR, to get the current firmware version. Before FOTA, version is BHL85xx.5.14.1.5.2.20171124.x6255
* Check APN settings
* Check indication settings, all indications are activated (8191)
* In this example, user agreement for “download” is deactivated, but activated for “install”
* Start DM session
* +WDSI:9 indicates that a package is available for download, and the package size is 2560 bytes (delta package)



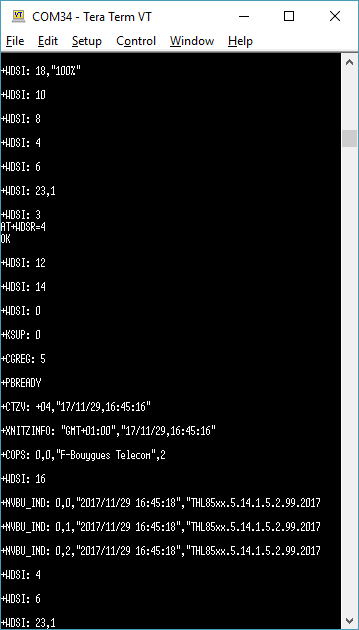
* +WDSI:18 indicates the download progress
* On AirVantage portal, the “Install application“ is now in progress



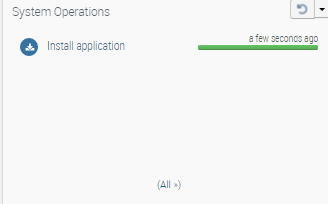
* The detail of this operation shows that the device has accepted the FOTA command



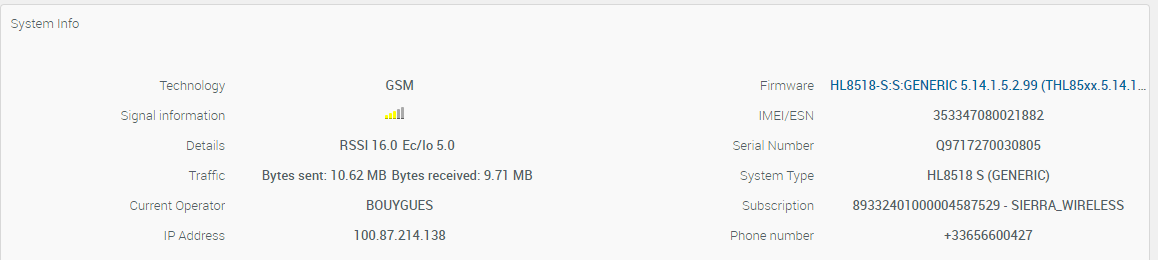
* +WDSI:18,”100%” indicates the download operation is reaching 100%
* +WDSI:10 indicates that package has been successfully downloaded and stored in flash
* +WDSI:3 indicates that the module is requesting user agreement to install the firmware package
* AT+WDSR=4 command has been entered to accept the package installation
* The installation process starts verifying the download package (authentication and integrity checks). +WDSI:12 indicates the package passed these verifications
* +WDSI:14 indicates the firmware update is being launched
* Upon install completion the module reboots
* +WDSI:16 indicates that the module has successfully started with the new firmware
* +NVBU\_IND:0,x indicate that all set of parameters corresponding to the new firmware have been backed up
* Per indications +WDSI:4, +WDSI:6 and +WDSI:23,1, the module connects to AirVantage to report the FOTA result
* AT+CGMR will confirm the new firmware being THL85xx.5.14.1.5.2.99.20171124.x6255
* Please note that the session remains active, therefore +WDSI:8 is not returned.



* On AirVantage portal, the FOTA operation now reflects a successful outcome



* The new firmware version as reported by the module, is also updated in the System Info widget



# Firmware Local Update

This section describes how to update the firmware locally without connecting to a remote DM server.

Firmware package (DWL file extension) must be available in the host. It could be a delta package or full package (not applicable to HL6).

AT+WDSD command is used to perform this update locally, as follow:

* Specify the size of the firmware to be downloaded by the module:

AT+WDSD=<dwl\_file\_size>

At this point, the module is waiting to receive data from the host. CME ERROR: 3 will occur if data transfer is not started within 5 minutes.

* Send the firmware package file to the module using 1K-XMODEM file transfer protocol. TeraTerm can be used to perform this file transfer. The file transfer must be initiated within 5 minutes.
* Upon completion of the file transfer, the module will be requesting a user agreement (+WDSI: 3) to install the firmware. To accept the installation:

AT+WDSR=4

* +WDSI:12 indicates that the downloaded package is valid
* +WDSI:14 indicates that the Update is about to be launched
* +WDSI:15 indicates that the downloaded package cannot be applied due to version mismatching
* If no firmware mismatch, +WDSI:16 will indicate the completion of the update. New firmware version can be checked with AT+CGMR.

# APN

## APN defined by WDSS

The module uses the APN defined by AT+WDSS to do the PDP activation for the bearer connection:

AT+WDSS=0,”your-apn”,”apn-login”,”apn-password”

The above APN setting will be copied onto CGDCONT’s cid#5 upon starting the connection (AT+WDSS=1,1) :

AT+WDSS=0,"a2bouytel.com"

OK

AT+WDSS?

+WDSS: 0,"a2bouytel.com",,5

+WDSS: 1,0

OK

AT+CGDCONT?+CGDCONT: 1,"IP","mmsbouygtel.com","10.79.116.105",0,0,0,0,0,0

OK

AT+WDSS=1,1OK

+WDSI: 4

+WDSI: 6

+WDSI: 23,1

AT+CGDCONT?+CGDCONT: 1,"IP","mmsbouygtel.com","10.79.116.105",0,0,0,0,0,0

+CGDCONT: 5,"IP","a2bouytel.com","10.62.176.69",0,0,0,0,0,0

OK

If the APN defined with WDSS is not valid, depending of the WDSM configuration (refer to Figure 9) the module may browse and try to use APN defined in CGDCONT, or just give up the connection to AirVantage.

## APN not defined by WDSS

In case AVMS APN has not been defined, AT+WDSM can define the APNs in CGDCONT to be used instead. Refer to below Figure 9.

AT+WDSS?

+WDSS: 0,""

+WDSS: 1,0

OK



1. AirPrime HL6 : Use of PDP context for DM connection

## APN Recommendation

It is recommended to have 2 APNs, contact your network provider to determine whether they can provide a second APN :

Dedicate a PDP context to AirVantage related services (i.e. FOTA and applicative data) : use WDSS to dedicate an APN or assign it with CGDCONT cid #5. Refer to §8.1

To avoid connection conflict and issue, your host application should be using the second APN for data connection. Use CGDCONT to assign the second APN to a cid other than #5.

If you only have one APN then you will not be able to initiate concurrent AirVantage service and data connection for your host application. You must manage connections using a shared APN. For instance, below are recommendations to manage the concurrent access :

* Assign the unique APN to cid #5 (CGDCONT=5,”IP”,<apn> or WDSS=1,0,<apn>)
* Before initiating AirVantage service (WDSS=1,1) make sure that PDP context cid#5 is not activated (CGACT?)
* Close AirVantage connection (WDSS=1,0) if it is not being used (no FOTA request or server request), so that host application data connection can be initialized
* Before initiating host application data connection make sure that AirVantage connection is not active (WDSS?) and monitor notifications of connection status changes (e.g. +WDSI:8)
* Close host application data connection if it is not being used so that AirVantage connection can be initiated

# Suspending and Resuming Download

An ongoing download operation can be suspended then resumed as follow:

+WDSI: 18, 5%

+WDSI: 18, 6%

AT+WDSS=1,0  // stopping the bearer, the package download is suspended

OK

…

…

AT+WDSS=1,1   // Will resume the package download

OK

+WDSI: 18, 7%

+WDSI: 18, 8%

AT+WDSS=1,0 stops the bearer for DM only (cid#5 by default for HL7 & HL8).

In the case where DM is using cid#1 (refer to §0), AT+WDSS=1,0 does not deactivate PDP cid#1. The network registration is maintained by PDP cid#1, if this latter is deactivated, the module will deregistered from the network.

AT+WDSS? returns +WDSS:1,x, where x indicates the status of the bearer: 0 for stopped, 1 for opened.

# Error Cases

This section lists the most common errors:

* The device is connected to DM server (+WDSI:23,1) however the module does not receive FOTA command created on AirVantage. This is due to the NAT being released by the mobile operator, therefore AirVantage can no longer send command to the device, as the external IP address and the port of the module is no longer valid (address translation being dropped). Downstream communication is therefore broken, however the connection remains active and the module is still able to send data to AirVantage. The inactivity period for the network to release the NAT is operator-dependant and can vary. Both the module and the AirVantage server are not aware of the NAT being released by the network.

To reestablish the downstream communication, the host processor can have the module to perform a LwM2M registration again, this can be achieved by issuing AT+WDSS=1,1. Sending upstream data will have the network to renew the NAT for the device, and AirVantage will update the new external IPaddress/Port of the device. The first AT+WDSS=1,1 actually opens the connection to AirVantage. Subsequent WDSS=1,1 does not create new connection but reused the existing connection to send registration request :

If the NAT is still active, AT+WDSS=1,1 just returns OK.

If the NAT has been released, AT+WDSS=1,1 returns OK, and +WDSI:4 is also returns to indicate a reconnection with handshaking to the server.

Note that sending application data (AT+AVDATA\* commands) to AirVantage also helps to update or maintain the NAT

* DM connection error (AT+WDSS=1,1)

+CME ERROR: 650, DM APN is not defined, or there is a pending operation (e.g. +WDSI: 2 or +WDSI: 3) that is waiting for an user agreement to be entered (AT+WDSR)

+CME ERROR: 133, Invalid APN

+CME ERROR: 148, Activation error

+WDSI: 7, connection error with DM server, try AT+WDSS=1,1 again

* Firmware update error:

+WDSI: 15, firmware update failed

This failure occurs when trying to do upgrade with a delta of mismatched firmware.

# Power cut

Ongoing FOTA operation (e.g. FW package download or FW Upgrade) will be resumed in case of power off/on. WDSI indications will be available after reset. And the pending user agreement will also be resumed.

# Fallback & Recovery

The module can revert back to the previous firmware only if the lastly updated package contains a reverse delta. This Fallback can be triggered using AT+WDSF or automatically in case of reset loop detection.

## Intentional fallback

To revert to the previous firmware, first check for the availability of the previous package :

AT+WDSF?

+WDSF: 1,X //X (0 or 1) indicates the availability of previous package

If X is 1 then it is possible to revert to the previous firmware, as follow:

AT+WDSF=1

+WDSI:17,1 indicates that the fallback has been performed and was initiated by the user.

## Automatic Recovery

The firmware could be reverted back to the previous version automatically in case of repetitive module reset (e.g. firmware malfunction). This can only be performed if a previous firmware package or delta is available.

The automatic recovery mechanism is triggered upon 5 consecutive resets. The reset counter is incremented on module reset occurring with 20 seconds after reboot. When this counter reaches 5 and a previous firmware package/delta is available then the fallback will be triggered automatically. There is no AT command indication for the reset loop detection. +WDSI:17,0 indicates that the fallback has been performed and was initiated automatically upon reset loop detection.

# Document History

|  |  |  |
| --- | --- | --- |
| **Level** | **Date** | **History** |
| 1.0 | January 15, 2018 | Creation |

# Legal Notice

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where cellular modems are not advised without proper device certifications. These areas include environments where cellular radio can interfere such as explosive atmospheres, medical equipment, or any other equipment which may be susceptible to any form of radio interference. The Sierra Wireless modem can transmit signals that could interfere with this equipment. Do not operate the Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator’s control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitations of Liability

This manual is provided “as is”. Sierra Wireless makes no warranties of any kind, either expressed or implied, including any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. The recipient of the manual shall endorse all risks arising from its use.

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Customer understands that Sierra Wireless is not providing cellular or GPS (including A-GPS) services. These services are provided by a third party and should be purchased directly by the Customer.

SPECIFIC DISCLAIMERS OF LIABILITY: CUSTOMER RECOGNIZES AND ACKNOWLEDGES SIERRA WIRELESS IS NOT RESPONSIBLE FOR AND SHALL NOT BE HELD LIABLE FOR ANY DEFECT OR DEFICIENCY OF ANY KIND OF CELLULAR OR GPS (INCLUDING A-GPS) SERVICES.

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product includes technology licensed from QUALCOMM®.

This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group and MMP Portfolio Licensing.

Copyright

© 2016 Sierra Wireless. All rights reserved.

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage®, WISMO®, ALEOS® and the Sierra Wireless and Open AT logos are registered trademarks of Sierra Wireless, Inc. or one of its subsidiaries.

Watcher® is a registered trademark of Netgear, Inc., used under license.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.