



Myriota

Myriota

AssetHawk™

Message Format

Description

XAN1110-04

August 2026

©Myriota Pty Ltd

Revision History

Rev	Date	Description of Change
01	Jan 2026	Initial version
02	Apr 2026	Added Tamper message reason Added Message Flag Detail Added BLE message format
03	Jun 2026	Changed the Terminal ID to the SIM ICCID Added the AssetHawk Serial number field to all messages Added the Transport field to all messages
04	Aug 2026	Updated for firmware v1.2.0 Expanded the Message Flag description Added Message Delivery and Ordering

Related Documentation

Find the latest versions of all Myriota documentation at developer.myriota.com

How to Contact Us

Technical Support

developer.myriota.com

support.myriota.com

Sales Support

sales@myriota.com

Myriota Online

myriota.com

Disclaimer

The information contained in this document (collectively, the “Information”) is provided to you (both the individual receiving this document and any legal entity on behalf of which such individual is acting) (“You” and “Your”) by Myriota Pty Ltd for information purposes only.

- Information in this document is provided solely to enable system and software implementers to use Myriota Pty Ltd products.
- Myriota Pty Ltd reserves the right to make changes without further notice to any products herein.
- You are responsible for making Your own assessments concerning the Information and Myriota recommends that You assess the accuracy, completeness and relevance of the Information for Your purposes before using or relying on any of the Information.
- Myriota is providing the Information to you “AS IS” and without regard to Your specific requirements.
- Myriota has exercised reasonable care in preparing the Information, however Myriota does not warrant the accuracy, completeness or relevance of the Information and accepts no liability for any errors or omissions in the Information.
- You acknowledge and agree that Your use of the Information is at your sole risk and that to the extent permitted by law Myriota is not liable for any loss or damage of whatever nature (direct, indirect, consequential or other) that arises in any way from Your use of or reliance on the Information.
- For further information, see myriota.com or contact your Myriota sales representative.

Table of Contents

Overview	5
Message Delivery and Ordering	5
POST request structure	5
Payload Format	9
Location Message	9
Location Payload Breakdown	9
Bluetooth Message	12

Overview

This document details the data structure of the messages from AssetHawk™ devices, which will be sent via HTTPS POST requests to customer visualisation platforms. The data received by the destination platform is in standard JSON format.

The payload contains telemetry data from the AssetHawk™, including location, device health (battery and temperature), and the specific reason the report was triggered (e.g., movement detected, stationary timeout, etc.).

Note that messages may be duplicated and/or arrive out of order.

Message Delivery and Ordering

AssetHawk delivers its messages via the Myriota HyperPulse NTN satellite network. Messages are stored on the device and forwarded when it next connects to a satellite, which impacts the final visualisation platform in the following ways:

1. Messages may arrive out of order.
2. Messages may be duplicated.
3. Messages often arrive in batches. Several messages may be delivered together after a period of silence.
4. Arrival time is not event time. Always use the `time` field inside the payload, not the POST request `Timestamp`, to place an event on a timeline.
5. Older messages may be discarded. The device buffers a limited number of messages, and the oldest are dropped in favour of the newest.

Use the payload `time` field together with the `Sequence Number` to order and de-duplicate messages. Note that each message type maintains its own independent sequence number series.

POST request structure

The body of the POST request is formatted as JSON. The example below illustrates the structure of the request.

```
{  
  "EndpointRef": "N_HlFTNgRsqh:uyXKvYTmTAO5.",  
  "time": "2017-01-01T00:00:00Z",  
  "lat": 42.331437,  
  "lon": -71.055777,  
  "alt": 10,  
  "speed": 0,  
  "battery": 100,  
  "temp": 25,  
  "reason": "stationary_timeout",  
  "sequence": 1  
}
```

```
"Timestamp": 1563521870,  
"Data":  
  "{  
    \"Packets\":  
      [{  
        \"Timestamp\": 1563521870359,  
        \"TerminalId\": \"89884380001010337013\",  
        \"Value\": \"MessagePayload\",  
        \"SerialNumber\": \"X99A25431234\",  
        \"Transport\": \"NTN\"}]  
      },  
    \"Id\": \"fe77e2c7-8e9c-40d0-8980-43720b9dab75\",  
    \"CertificateUrl\": \"https://security.myriota.com/data-13f71.crt\",  
    \"Signature\": \"k2OIBppBXmBT520rUllvMxNg+h9soJYBhQhOGSIWGdzkppdT1..\"  
  }  
}
```

The table below provides a breakdown of the corresponding fields in the POST request.

Field	Type	Description																		
EndpointRef	String	Unique Identifier of the destination																		
Timestamp	Number	Unix Epoch time at which the HTTP POST request was generated																		
Data	Object	A JSON serialised structure with the following fields: <table> <tr> <td>Packets</td><td>List</td><td>JSON list of the packets received from the device. For AssetHawk, this list only contains one message.</td></tr> <tr> <td>Timestamp</td><td>Number</td><td>Unix Epoch time (ms) at which the packet was captured by the satellite</td></tr> <tr> <td>TerminalId</td><td>Number</td><td>SIM card ICCID from which the packet was transmitted</td></tr> <tr> <td>Value</td><td>Object</td><td>The payload data from the device. See Payload Format for more information.</td></tr> <tr> <td>SerialNumber</td><td>Text</td><td>The Serial number of the AssetHawk device from which the packet was sent.</td></tr> <tr> <td>Transport</td><td>Text</td><td> The network technology through which the message was delivered. - TN = Cellular - NTN = Satellite </td></tr> </table>	Packets	List	JSON list of the packets received from the device. For AssetHawk, this list only contains one message.	Timestamp	Number	Unix Epoch time (ms) at which the packet was captured by the satellite	TerminalId	Number	SIM card ICCID from which the packet was transmitted	Value	Object	The payload data from the device. See Payload Format for more information.	SerialNumber	Text	The Serial number of the AssetHawk device from which the packet was sent.	Transport	Text	The network technology through which the message was delivered. - TN = Cellular - NTN = Satellite
Packets	List	JSON list of the packets received from the device. For AssetHawk, this list only contains one message.																		
Timestamp	Number	Unix Epoch time (ms) at which the packet was captured by the satellite																		
TerminalId	Number	SIM card ICCID from which the packet was transmitted																		
Value	Object	The payload data from the device. See Payload Format for more information.																		
SerialNumber	Text	The Serial number of the AssetHawk device from which the packet was sent.																		
Transport	Text	The network technology through which the message was delivered. - TN = Cellular - NTN = Satellite																		
Id	String	HTTPS Message UUID																		

CertificateUrl	URL	URL of certificate containing the public key to authenticate the Signature.
Signature	String	PKCS1_15 signature of Timestamp, Id and Data fields

Details on how to use the Certificate and Signature fields to validate the data are outlined on the Myriota Support site [here](#).

Payload Format

Location Message

The payload data is in JSON format, as shown in the example location payload data below:

```
"Value": {  
  "type": 1,  
  "sequence_number": 10,  
  "reason": 0,  
  "flags": 2,  
  "time": 1738183958,  
  "latitude": -34.9275233,  
  "longitude": 138.6075245,  
  "elevation": 63.032,  
  "temperature": 18,  
  "battery_voltage": 3.600  
}
```

Location Payload Breakdown

The table below describes each field in the JSON location payload and its unit of measurement (UOM).

Content	UOM	Note						
Message Type	N/A	Message versioning tracks changes to the message structure. <table><tr><th>Value</th><th>Description</th></tr><tr><td>1</td><td>Location Message</td></tr><tr><td>8</td><td>Bluetooth Message</td></tr></table>	Value	Description	1	Location Message	8	Bluetooth Message
Value	Description							
1	Location Message							
8	Bluetooth Message							
Sequence Number	N/A	An incrementing number to keep track of the message sequence, i.e. message count. The						

		sequence number has a maximum value of 255; after that, it wraps around to 0 and continues counting. If this number resets to 0 before reaching 255, the device has reset/rebooted. This number is increased separately for each Message Type.																		
Message Reason		The reason the message was sent. The reason is specified as a number (enumeration). The table below defines each value. <table><tr><th>Value</th><th>Description</th></tr><tr><td>0</td><td>The first message sent after boot. Triggered ~60 seconds after startup.</td></tr><tr><td>1</td><td>Stationary interval elapsed: the device has been stationary for the configured stationary interval.</td></tr><tr><td>2</td><td>Movement started: the device was stationary, and movement has now been detected.</td></tr><tr><td>3</td><td>Movement stopped: the device was in motion and has since stopped.</td></tr><tr><td>4</td><td>Movement interval elapsed: The device was in motion and remains in motion.</td></tr><tr><td>5</td><td>Reserved for future use.</td></tr><tr><td>6</td><td>The device has been tampered with. Sent once when tamper is first detected.</td></tr><tr><td>7</td><td>Alert interval elapsed: an ongoing report while the device remains in the alerted state.</td></tr></table>	Value	Description	0	The first message sent after boot. Triggered ~60 seconds after startup.	1	Stationary interval elapsed: the device has been stationary for the configured stationary interval.	2	Movement started: the device was stationary, and movement has now been detected.	3	Movement stopped: the device was in motion and has since stopped.	4	Movement interval elapsed: The device was in motion and remains in motion.	5	Reserved for future use.	6	The device has been tampered with. Sent once when tamper is first detected.	7	Alert interval elapsed: an ongoing report while the device remains in the alerted state.
Value	Description																			
0	The first message sent after boot. Triggered ~60 seconds after startup.																			
1	Stationary interval elapsed: the device has been stationary for the configured stationary interval.																			
2	Movement started: the device was stationary, and movement has now been detected.																			
3	Movement stopped: the device was in motion and has since stopped.																			
4	Movement interval elapsed: The device was in motion and remains in motion.																			
5	Reserved for future use.																			
6	The device has been tampered with. Sent once when tamper is first detected.																			
7	Alert interval elapsed: an ongoing report while the device remains in the alerted state.																			
Message Flag	N/A	A single byte carrying two separate pieces of information. The first four bits report the device's state when the message was created, and more																		

		than one may apply at once. The upper 4 bits report reserved information. <table><tr><th>Bit Number</th><th>Description</th></tr><tr><td>0</td><td>0 = Correct device orientation 1 = Incorrect device orientation</td></tr><tr><td>1</td><td>0 = Valid GPS Fix in the message 1 = The GPS fix in the message is stale (last known values)</td></tr><tr><td>2</td><td>0 = Not in a tampered state 1 = In a tampered state</td></tr><tr><td>3</td><td>Reserved for future use</td></tr></table>	Bit Number	Description	0	0 = Correct device orientation 1 = Incorrect device orientation	1	0 = Valid GPS Fix in the message 1 = The GPS fix in the message is stale (last known values)	2	0 = Not in a tampered state 1 = In a tampered state	3	Reserved for future use
Bit Number	Description											
0	0 = Correct device orientation 1 = Incorrect device orientation											
1	0 = Valid GPS Fix in the message 1 = The GPS fix in the message is stale (last known values)											
2	0 = Not in a tampered state 1 = In a tampered state											
3	Reserved for future use											
Time	N/A	The time of the location reading, in UTC . This is in Unix time format (also called Epoch time). e.g. 1758520800 is 2025-09-22 06:00:00										
Latitude	degrees	The device's latitude in degrees.										
Longitude	degrees	The device's longitude in degrees.										
Elevation	m	The device's elevation above average sea level, in meters.										
Temperature	°C	Internal temperature of the device in degrees Celsius										
Battery Voltage	V	The device's battery level in Volts.										

Note: Future firmware releases may add additional fields, reasons and/or flags to the payload data structure

Bluetooth Message

The payload data is in JSON format, as shown in the example BLE payload data below:

```
"Value": {  
  "type": 8,  
  "sequence_number": 10,  
  "time": 1738183958,  
  "protocol": 1,  
  "RSSI": -70,  
  "address": "AA:BB:CC:DD:EE:FF",  
  "data": "Beacon Data"  
}
```

The table below describes each field in the JSON BLE payload and its unit of measurement (UOM).

Content	UOM	Note						
Message Type	N/A	Message versioning tracks changes to the message structure. <table><tr><th>Value</th><th>Description</th></tr><tr><td>1</td><td>Location Message</td></tr><tr><td>8</td><td>Bluetooth Message</td></tr></table>	Value	Description	1	Location Message	8	Bluetooth Message
Value	Description							
1	Location Message							
8	Bluetooth Message							
Sequence Number	N/A	An incrementing number to keep track of the message sequence, i.e. message count. The sequence number has a maximum value of 255; after that, it wraps around to 0 and continues counting. If this number resets to 0 before reaching 255, the device has reset/rebooted. This number is increased separately for each Message Type.						

Time	ms	The time in milliseconds from boot that the BLE message was received..	
Protocol	N/A	BLE advertising protocol type from the beacon.	
		Value	Description
		0	EddyStone format
		1	Reserved for future use
		2	Reserved for future use
		3	Advertising data or scan response frame
RSSI	dBm	Signal strength between the AssetHawk and the BLE beacon in dBm.	
Address	N/A	MAC address of the beacon.	
Data	N/A	Raw beacon payload. The beacon payload is not decoded and is sent as captured from the beacon.	

Note: Future firmware releases may add additional fields, reasons and/or flags to the payload data structure