

# Webhooks End User Documentation

## Overview

Aerohive provides a [Webhooks](#) API that allows registered subscribers to receive HTTPS callbacks when specific events occur. Today, the supported events are related to Location/Presence. In the future, we plan to expand the events to include monitoring and other data.

In contrast, to Aerohive's [RESTful](#) APIs, where users explicitly pull data from Aerohive's services, Webhooks push data to a customer's endpoint that is registered to receive these messages. All messages are gzip encoded. Normally, your web server will transparently handle the gzip encoding. If not you may have to configure your web server or application.

## Webhooks Callback Registration

Subscription to Webhooks requires registration. Required information includes:

Attribute	Data Type	Discussion
ownerId	Number/Long	The ownerId associated with your Aerohive account. You can view this information in the About dialog in Hive Manager NG. This is also known as the VHM-Id.
application	String	The name of your application.
secret	String	A secret value sent to your application within an <a href="#">HTTP Authorization</a> header.
url	String	The HTTPS URL to which the callback message is being sent. HTTPS is required.
eventType	String	The type of event to register for, current supported values include only "LOCATION".
messageType	String	The message schema to register for, current supported values include only "LOCATION_AP_CENTRIC" and "LOCATION_CLIENT_CENTRIC".

Registration can be accomplished using a UI [tool](#) or directly using the [REST API](#). In addition to registration, Aerohive also needs to explicitly register your account for location and presence analytics. Please send an email to [Developer.Portal@aerohive.com](mailto:Developer.Portal@aerohive.com) with your ownerId and a screen shot of your About page in Hive Manager.

# HTTP Headers

In all webhook callback messages, Aerohive supplies the following HTTP Headers.

HTTP Header	Discussion
Authorization	The standard <a href="#">HTTP Authorization</a> header is provided with the following value:  "Basic " + the secret value provided to Aerohive when registering for the web hook callback. This value is not BASE 64 encoded.
X-AH-Event-Type	The Event Type (e.g. "LOCATION") that triggered the callback.
X-AH-Message-Type	The Message Type, or Message Schema, associated with the message. For example, "LOCATION_AP_CENTRIC" or  "LOCATION_CLIENT_CENTRIC".

By the use of these HTTP Headers, a subscriber can multiplex across different messages on a single endpoint.

## Location/Presence Events

Aerohive currently provides two message schemas related to Location/Presence events:

1. AP Centric (LOCATION\_AP\_CENTRIC)
2. Client Centric (LOCATION\_CLIENT\_CENTRIC)

All Location/Presence callbacks occur at approximately one minute intervals.

### AP Centric

The AP Centric message schema is provided mostly for backwards compatibility with prior releases. This message schema has been deprecated and will be removed in a future release. Some minor changes are included to make the Webhook message schema compatible with the external API. An AP Centric message is sent for each Access Point that observes client devices. If a client device is observed by multiple access points, information about that client device will appear in multiple messages, one for each AP that observes that device. It's for this

reason that this message schema is being deprecated and removed. It does not scale for customers with high density environments.

The following shows a sample AP Centric message.

### **Sample AP Centric Webhook Message**

```
{
  "messageMetadata" : {
    "eventType" : "LOCATION",
    "messageType" : "LOCATION_AP_CENTRIC"
  },
  "data" : {
    "ownerId" : "1001",
    "apMac" : "3c9c076106bf",
    "locationIDHierarchy" : [ 1, 2, 3, 4 ],
    "observations" : [ {
      "clientMac" : "92dd7a6da28f",
      "ipv4" : "11.252.222.184",
      "ipv6" : null,
      "seenTime" : "2016-11-04T19:55:46.033Z",
      "seenEpoch" : 1478289346033,
      "userName" : "Sam",
      "authMethod" : "WPA2_8021X",
      "ssid" : "My SSID",
      "manufacturer" : "Apple",
      "os" : "IOS6",
      "lat" : 45.0,
      "lng" : 111.0,
      "x" : 0.0,
      "y" : 0.0,
      "clientMetadata" : {
        "locationCalcMethod" : "TRILATERATION",
        "locationError" : null,
        "randomizedMac" : false
      },
      "rssi" : -63
    }, {
      "clientMac" : "16c4420bd636",
      "ipv4" : "99.16.150.175",
      "ipv6" : null,
      "seenTime" : "2016-11-04T19:55:46.033Z",
      "seenEpoch" : 1478289346033,
      "userName" : "Harry",
      "authMethod" : "WPA2_8021X",
      "ssid" : "My SSID",
      "manufacturer" : "Apple",
      "os" : "IOS6",
      "lat" : 45.0,
      "lng" : 111.0,
      "x" : 0.0,
      "y" : 0.0,
    }
  ]
}
```

```

    "clientMetadata" : {
      "locationCalcMethod" : "TRILATERATION",
      "locationError" : null,
      "randomizedMac" : false
    },
    "rssi" : -63
  } ]
}

```

The following tables describes the JSON message body on an individual element basis.

Element				
messageMetadata	This element contains information about the message being received. Note that this data is also sent as <a href="#">HTTP Headers</a> .	<b>Element</b>	<b>Data Type</b>	<b>Discussion</b>
		eventType	String	The type of event that triggered this Webhook callback. The value 'LOCATION' indicates that a Location/Presence event was the trigger.
		messageType	String	The schema of message being delivered. The value 'LOCATION_AP_CENTRIC' indicates that the AP Centric Location schema message is being delivered.

Element				
data	An envelope for the payload of the message. This envelope is provided for compatibility with the external REST API.	Element	Data Type	Discussion
		ownerId	Number/Long	The unique customer identifier.
		apMac	String	The MAC Address of the Access Point for which this message is being sent.
		locationIDHierarchy	Array of Number/Long	The location folder path of this Access Point with respect to the customer defined Building/Floor folder hierarchy. The last mode in the array is the leaf node in the hierarchy. To obtain the labels associated with these numeric location ids, the ../configuration/apLocationFolders REST endpoints are available.

observations	An array of JSON objects, one instance for each client observation. If multiple observations of the client device are recorded within the reporting period, only the most recent observation is reported.	<table border="1"> <thead> <tr> <th>Element</th> <th>Data Type</th> <th>Discussion</th> </tr> </thead> <tbody> <tr> <td>clientMac</td> <td>String</td> <td>The <a href="#">MAC Address</a> of the client device as observed by the access point. Note that this could be a randomized MAC Address, see the <a href="#">clientMetadata</a> element for further discussion.</td> </tr> <tr> <td>ipv4</td> <td>String</td> <td>The <a href="#">IPv4</a> address of this client device. This attribute will be null when the client devices is not associated with the access point.</td> </tr> <tr> <td>ipv6</td> <td>String</td> <td>The <a href="#">IPv6</a> address of the client device. This attribute will be null when the client device is not associated with the access point.</td> </tr> <tr> <td>seenTime</td> <td>String</td> <td>The timestamp, in <a href="#">ISO-8601</a> format, that the client device was observed by the access point. The format 2016-09-30T19:48:00.269Z is used for all ISO-8601 date time values and all date time values will be <a href="#">UTC</a>.</td> </tr> <tr> <td>seenEpoch</td> <td>Number/Long</td> <td>The <a href="#">UNIX Epoch</a> timestamp that the client devices was observed by the access point.</td> </tr> <tr> <td>userName</td> <td>String</td> <td>For client devices that associated with the WiFi network, this attribute will contain the identity information used to authenticate. For an unassociated client device, this attribute will be null.</td> </tr> <tr> <td>authMethod</td> <td>String</td> <td>For authenticated client devices, this attribute will contain the method used for authentication. Valid values include: <table border="1"> <thead> <tr> <th>Auth Method</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CWP</td> <td><a href="#">Captive Web Portal</a></td> </tr> </tbody> </table> </td> </tr> </tbody> </table>	Element	Data Type	Discussion	clientMac	String	The <a href="#">MAC Address</a> of the client device as observed by the access point. Note that this could be a randomized MAC Address, see the <a href="#">clientMetadata</a> element for further discussion.	ipv4	String	The <a href="#">IPv4</a> address of this client device. This attribute will be null when the client devices is not associated with the access point.	ipv6	String	The <a href="#">IPv6</a> address of the client device. This attribute will be null when the client device is not associated with the access point.	seenTime	String	The timestamp, in <a href="#">ISO-8601</a> format, that the client device was observed by the access point. The format 2016-09-30T19:48:00.269Z is used for all ISO-8601 date time values and all date time values will be <a href="#">UTC</a> .	seenEpoch	Number/Long	The <a href="#">UNIX Epoch</a> timestamp that the client devices was observed by the access point.	userName	String	For client devices that associated with the WiFi network, this attribute will contain the identity information used to authenticate. For an unassociated client device, this attribute will be null.	authMethod	String	For authenticated client devices, this attribute will contain the method used for authentication. Valid values include: <table border="1"> <thead> <tr> <th>Auth Method</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CWP</td> <td><a href="#">Captive Web Portal</a></td> </tr> </tbody> </table>	Auth Method	Description	CWP	<a href="#">Captive Web Portal</a>
		Element	Data Type	Discussion																										
		clientMac	String	The <a href="#">MAC Address</a> of the client device as observed by the access point. Note that this could be a randomized MAC Address, see the <a href="#">clientMetadata</a> element for further discussion.																										
		ipv4	String	The <a href="#">IPv4</a> address of this client device. This attribute will be null when the client devices is not associated with the access point.																										
		ipv6	String	The <a href="#">IPv6</a> address of the client device. This attribute will be null when the client device is not associated with the access point.																										
		seenTime	String	The timestamp, in <a href="#">ISO-8601</a> format, that the client device was observed by the access point. The format 2016-09-30T19:48:00.269Z is used for all ISO-8601 date time values and all date time values will be <a href="#">UTC</a> .																										
		seenEpoch	Number/Long	The <a href="#">UNIX Epoch</a> timestamp that the client devices was observed by the access point.																										
		userName	String	For client devices that associated with the WiFi network, this attribute will contain the identity information used to authenticate. For an unassociated client device, this attribute will be null.																										
authMethod	String	For authenticated client devices, this attribute will contain the method used for authentication. Valid values include: <table border="1"> <thead> <tr> <th>Auth Method</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CWP</td> <td><a href="#">Captive Web Portal</a></td> </tr> </tbody> </table>	Auth Method	Description	CWP	<a href="#">Captive Web Portal</a>																								
Auth Method	Description																													
CWP	<a href="#">Captive Web Portal</a>																													

				<table border="1"> <tr> <td>OPEN</td> <td>The network required no authentication</td> </tr> <tr> <td>WEP</td> <td><a href="#">WEP</a> Open System</td> </tr> <tr> <td>WEP_SHARED</td> <td><a href="#">WEP</a> Shared Key</td> </tr> <tr> <td>WPA_PSK</td> <td><a href="#">WPA</a> Pre-Shared Key</td> </tr> <tr> <td>WPA2_PSK</td> <td><a href="#">WPA2</a> Pre-Shared Key</td> </tr> <tr> <td>WPA_8021X</td> <td>WPA with 802.1x authentication</td> </tr> <tr> <td>WPA2_8021X</td> <td>WPA2 with 802.1x authentication</td> </tr> <tr> <td>WPA_AUTOPSK</td> <td>WPA with Auto PSK</td> </tr> <tr> <td>WPA_AUTO8021X</td> <td>WPA with Auto PSK and 802.1x</td> </tr> <tr> <td>DYNAMIC_WEP</td> <td><a href="#">Dynamic WEP</a></td> </tr> </table>	OPEN	The network required no authentication	WEP	<a href="#">WEP</a> Open System	WEP_SHARED	<a href="#">WEP</a> Shared Key	WPA_PSK	<a href="#">WPA</a> Pre-Shared Key	WPA2_PSK	<a href="#">WPA2</a> Pre-Shared Key	WPA_8021X	WPA with 802.1x authentication	WPA2_8021X	WPA2 with 802.1x authentication	WPA_AUTOPSK	WPA with Auto PSK	WPA_AUTO8021X	WPA with Auto PSK and 802.1x	DYNAMIC_WEP	<a href="#">Dynamic WEP</a>
OPEN	The network required no authentication																							
WEP	<a href="#">WEP</a> Open System																							
WEP_SHARED	<a href="#">WEP</a> Shared Key																							
WPA_PSK	<a href="#">WPA</a> Pre-Shared Key																							
WPA2_PSK	<a href="#">WPA2</a> Pre-Shared Key																							
WPA_8021X	WPA with 802.1x authentication																							
WPA2_8021X	WPA2 with 802.1x authentication																							
WPA_AUTOPSK	WPA with Auto PSK																							
WPA_AUTO8021X	WPA with Auto PSK and 802.1x																							
DYNAMIC_WEP	<a href="#">Dynamic WEP</a>																							
		ssid	String	The <a href="#">SSID</a> that the client associated with.																				
		manufacturer	String	The manufacturer of the client device. This attribute will be null for unassociated client devices.																				
		os	String	The operating system of the client device. This device will be null if the client device is unassociated.																				
		lat	Number/Decimal	The latitude of the client device. See the clientMetadata element for interpretation.																				



Element				
		lng	Number/Decimal	The longitude of the client device. See the clientMetadata element for interpretation.
		x	Number/Decimal	The offset in meters, in the X coordinate space, from the origin of the floor plan. If the X and Y values are provided and the lat and lng elements are null, this generally means that your access point/device is not properly configured with a latitude and longitude.
		y	Number/Decimal	The offset in meters, in the Y coordinate space, from the origin of the floor plan. If the X and Y values are provided and the lat and lng elements are null, this generally means that your access point/device is not properly configured with a latitude and longitude.
		rssi	Number/Integer	The <a href="#">RSSI</a> value associated with this client as reported by the associated access point. The unit of measurement for the RSSI value is dBm. If multiple observations of the client occurred within the callback interval, the average RSSI value is used.

		<b>Element</b>	<b>Data Type</b>	<b>Discussion</b>								
		locationCalcMethod	String	<p>This attribute provides information regarding how the client positioned was calculated.</p> <p>The values and descriptions are shown in the following table:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>AP_LOCATION</td> <td>The client device was observed by only one access point and the derived location is equivalent to the configured location of that access point.</td> </tr> <tr> <td>MIDPOINT</td> <td>The client device was observed by only two access points and the derived location is equivalent to the midpoint between those two access points.</td> </tr> <tr> <td>TRILATERATION</td> <td>Three or more access points observed the client device and the location was derived using <a href="#">trilateration</a>.</td> </tr> <tr> <td>ERROR</td> <td>An error occurred, consult the locationError attribute for</td> </tr> </tbody> </table>	Value	Description	AP_LOCATION	The client device was observed by only one access point and the derived location is equivalent to the configured location of that access point.	MIDPOINT	The client device was observed by only two access points and the derived location is equivalent to the midpoint between those two access points.	TRILATERATION	Three or more access points observed the client device and the location was derived using <a href="#">trilateration</a> .
Value	Description											
AP_LOCATION	The client device was observed by only one access point and the derived location is equivalent to the configured location of that access point.											
MIDPOINT	The client device was observed by only two access points and the derived location is equivalent to the midpoint between those two access points.											
TRILATERATION	Three or more access points observed the client device and the location was derived using <a href="#">trilateration</a> .											
ERROR	An error occurred, consult the locationError attribute for											
clientMetadata	Additional metadata that aids in the interpretation of the derived location information for this client.											

Element				
				additional information.
		locationError	String	This attribute is non-null when an error occurred that prevented location calculation. The locationCalcMethod will also contain a value of ERROR under this condition.
		randomizedMac	boolean	A value of true indicates that the clientMac address is a randomized, locally administered MAC Address rather than the real globally administered address. A value of false indicates that at the clientMac attribute reflects the real MAC Address of the client device.

## Client Centric

The Client Centric message schema is a new message format that we believe will be more efficient and easier to process. Subscribers to the AP Centric message schema will receive multiple messages for a given client, one for each Access Point that observes that client. This is a lot of redundant information and requires specific processing on the received end to correlate client observations across access points. In contrast, the Client Centric schema presents a single view of a client device and shows the Access points that are observing that client device.

### Sample Client Centric Webhook Message

```
{
  "messageMetadata" : {
    "eventType" : "LOCATION",
    "messageType" : "LOCATION_CLIENT_CENTRIC"
  },
  "data" : {
    "ownerId" : "1001",
    "observations" : [ {
      "clientMac" : "b8d2d03ca2d4",
      "ipv4" : "47.113.226.140",
      "ipv6" : null,
      "seenTime" : "2016-11-04T19:56:11.322Z",
      "seenEpoch" : 1478289371322,
      "userName" : "Jack",
      "authMethod" : "WPA2_8021X",
      "ssid" : "My SSID",
      "manufacturer" : "Apple",
      "os" : "IOS6",
      "lat" : 45.0,
      "lng" : 111.0,
      "x" : 0.0,
      "y" : 0.0,
      "clientMetadata" : {
        "locationCalcMethod" : "TRILATERATION",
        "locationError" : null,
        "randomizedMac" : false
      },
      "deviceObservers" : [ {
        "apMac" : "924f03556098",
        "rssi" : -22,
        "locationIDHierarchy" : [ 1, 2, 3, 4 ]
      }, {
        "apMac" : "920f2c789477",
        "rssi" : -12,
        "locationIDHierarchy" : [ 1, 2, 3, 4 ]
      }, {
        "apMac" : "beb9f85771e4",
        "rssi" : -25,
        "locationIDHierarchy" : [ 1, 2, 3, 4 ]
      } ]
    }, {
      "clientMac" : "84e8479be8c0",
      "ipv4" : "147.98.222.207",
      "ipv6" : null,
      "seenTime" : "2016-11-04T19:56:11.329Z",
      "seenEpoch" : 1478289371329,
    } ]
  }
}
```

```
"userName" : "Evelyn",
"authMethod" : "WPA2_8021X",
"ssid" : "My SSID",
"manufacturer" : "Apple",
"os" : "IOS6",
"lat" : 45.0,
"lng" : 111.0,
"x" : 0.0,
"y" : 0.0,
"clientMetadata" : {
  "locationCalcMethod" : "TRILATERATION",
  "locationError" : null,
  "randomizedMac" : false
},
"deviceObservers" : [ {
  "apMac" : "6e51959153c0",
  "rssi" : -64,
  "locationIDHierarchy" : [ 1, 2, 3, 4 ]
}, {
  "apMac" : "f83c957ed6b1",
  "rssi" : -40,
  "locationIDHierarchy" : [ 1, 2, 3, 4 ]
}, {
  "apMac" : "8ee35a1036a9",
  "rssi" : -97,
  "locationIDHierarchy" : [ 1, 2, 3, 4 ]
} ]
}, {
  "clientMac" : "343ecd201ddf",
  "ipv4" : "199.188.29.248",
  "ipv6" : null,
  "seenTime" : "2016-11-04T19:56:11.330Z",
  "seenEpoch" : 1478289371330,
  "userName" : "Harry",
  "authMethod" : "WPA2_8021X",
  "ssid" : "My SSID",
  "manufacturer" : "Apple",
  "os" : "IOS6",
  "lat" : 45.0,
  "lng" : 111.0,
  "x" : 0.0,
  "y" : 0.0,
  "clientMetadata" : {
    "locationCalcMethod" : "TRILATERATION",
    "locationError" : null,
```

```

    "randomizedMac" : false
  },
  "deviceObservers" : [ {
    "apMac" : "98230c135256",
    "rssi" : -11,
    "locationIDHierarchy" : [ 1, 2, 3, 4 ]
  }, {
    "apMac" : "7cfcla9e4a4b",
    "rssi" : -70,
    "locationIDHierarchy" : [ 1, 2, 3, 4 ]
  }, {
    "apMac" : "c6a83df93968",
    "rssi" : -21,
    "locationIDHierarchy" : [ 1, 2, 3, 4 ]
  } ]
} ]
}
}

```

The [observations](#) element is almost the same for the Client Centric schema as the AP Centric schema. The difference is the lack of an rssi attribute in the Client Centric schema and the addition of the deviceObservers element, which includes the rssi attribute.

### Client Centric deviceObservers Element

```

"deviceObservers" : [ {
  "apMac" : "98230c135256",
  "rssi" : -11,
  "locationIDHierarchy" : [ 1, 2, 3, 4 ]
}, {
  "apMac" : "7cfcla9e4a4b",
  "rssi" : -70,
  "locationIDHierarchy" : [ 1, 2, 3, 4 ]
}, {
  "apMac" : "c6a83df93968",
  "rssi" : -21,
  "locationIDHierarchy" : [ 1, 2, 3, 4 ]
} ]

```

Each instance of a client device observation will include a deviceObservers element that shows the information about the access points observing that client device.

Element	Data Type	Discussion									
deviceObservers	Object	One instance per access point/device observing the client device.									
		<table border="1"> <thead> <tr> <th>Element</th> <th>Data Type</th> <th>Discussion</th> </tr> </thead> <tbody> <tr> <td>apMac</td> <td>String</td> <td>The MAC Address of the Access Point/device that observed this client device.</td> </tr> <tr> <td>rssI</td> <td>Number/Integer</td> <td>The <a href="#">RSSI</a> value associated with this client as reported by the associated access point.</td> </tr> </tbody> </table>	Element	Data Type	Discussion	apMac	String	The MAC Address of the Access Point/device that observed this client device.	rssI	Number/Integer	The <a href="#">RSSI</a> value associated with this client as reported by the associated access point.
		Element	Data Type	Discussion							
apMac	String	The MAC Address of the Access Point/device that observed this client device.									
rssI	Number/Integer	The <a href="#">RSSI</a> value associated with this client as reported by the associated access point.									

## Recommended Architecture for Webhook Consumption

Due to the frequency of callbacks and the potential large message size, we recommend that customers consume the messages in an asynchronous fashion and decouple the endpoint from the consumer using a message queue. This will allow message delivery to complete as quickly as possible and maintain a high service level for all customers. If your application does not return an HTTP response code in 5 seconds or less, a timeout will occur.

## Message Schema Evolution

You can expect the schemas associated with the webhook messages to change. We will always attempt to maintain backwards compatibility and not break existing consumers.

The following sections describe the definition of backwards compatibility and non-backwards compatibility.

### Changes That Are Considered To Be Backwards Compatible

The following table describes changes that can be expected and are considered to be backwards compatible.

<b>Change</b>	<b>Discussion</b>
Adding New Elements	Adding a new attribute or element to the body of the JSON message is considered to be backwards compatible. If your implementation breaks when a new JSON element is added, you need to reconsider your implementation.
Adding New Enumerated Values	Adding a new enumerated/allowable value to an existing attribute.

## Changes That Are Considered To Be Non-Backwards Compatible

We will avoid non-backwards compatible changes to JSON Message schemas whenever possible. The following table describes changes that are considered to be non-backwards compatible.

<b>Change</b>	<b>Discussion</b>
Removing Elements	Removing an attribute or element.
Enumeration Changes	Changing the list of enumerated/allowable values for a message body where one of the prior accepted values is no longer acceptable.
Data Type Changes	Changing the type (e.g. from String to Number or vice-versa) of an attribute in a JSON message body.  The same applies when changing the Data Type from a simple type to an array type and vice-versa.
Name Change	Changing the name of an element or attribute is equivalent to removing an attribute or element.



From Chris: new AP centric message

```
{"messageMetaData":
  {
    "eventType":"LOCATION",
    "messageType":"LOCATION_AP_CENTRIC"
  },
  "data":
    {
      "ownerId":102,
      "apDevices":
        [
          {
            "apMac":"885BDD6A9D00",
            "locationIdHierarchy":[
              438086764294,
              438086764293,
              438086764291,
              438086764289],
            "observations":[
              {
                "clientMac":"60F81DC41952",
                "ipv4":?"10.1.1.1",
                "ipv6":null,
```

"seenTime":"2018-04-16T13:10:48.806-04:00",

"seenEpoch":1523898648806,

"userName":"no-name",

"authMethod":"wpa2-8021x",

"ssid":"myssid",

"manufacturer":"Apple",

"os":"IOS6",

"lat":0.0,

"lng":0.0,

"x":84.9424778761062,

"y":31.11061946902655,

"clientMetaData":null,

"rssi":-75},

{

"clientMac":"3CA9F455FF38",

"ipv4":null,

"ipv6":null,

"seenTime":"2018-04-16T13:10:10.367-04:00",

"seenEpoch":1523898610367,

"userName":null,

"authMethod":null,

"ssid":null,

```
"manufacturer":null,  
"os":null,  
"lat":0.0,  
"lng":0.0,  
"x":84.9424778761062,  
"y":31.11061946902655,  
"clientMetaData":null,"rsi":-67}
```

```
]
```

```
}
```

```
]
```

```
}
```

```
}
```