FORTINET
High Performance Network Security

# Fortinet Push API for FortiPresence

**VERSION 1**

**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**FORTICAST**

http://forticast.fortinet.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

August 30, 2017

Fortinet Push API for FortiPresence

01-246290-20170830

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2017-08-30 | Initial release. |

# Overview

The following document defines a API for presence analytics messages to be posted to services such as Fortipresence or 3rd party. This API allows each FAP accesspoint to forward station update messages directly to presence analytics collector without the need to go through the FortiGate, FortiWLC, or FortiCloud.

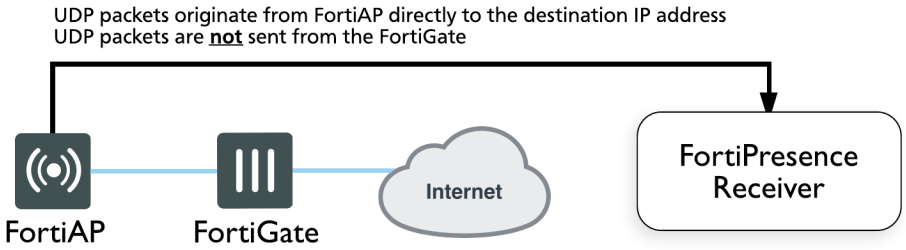
## Motivation: Pull versus Push API

Import based on Pull API turned out to be hard to setup, maintain and a constant security concern. The Push API idea is based on a regular Access Point Report in format below delivered via UDP datagrams.

# Architecture

Please note that in this architecture the UDP packets originate from the FAP or FAP-S to destination IP and NOT from FortiGate controller.

In Version 0.8 update, additional headers are added to support push from FortiGate or FortiWLC as well.



# Configuring the FortiGate and FortiPresence API

Navigate to the AP profile and find the RTLS settings. Please note that there are two different RTLS server configuration sections. There is the standard feed, RTLS Server Configuration, and an Aeroscout specific feed, AeroScout RTLS. The standard FortiPresence feed is what should be used by 3rd party partners.

## Configuring the FortiGate

Fortinet Development: Please create a 2nd LBS option for FortiPresence.

You need to configure:

| | |
|---|---|
| fortipresence-server | FortiPresence server IP address or name |
| fortipresence-port | FortiPresence server UDP listening port (the default is 3000) |
| fortipresence-secret | FortiPresence secret password (8 characters maximum) |
| fortipresence-project | FortiPresence project name (16 characters maximum) |
| fortipresence-frequency | FortiPresence report transmit frequency (Range 5 to 65535 seconds. Default = 30) |
| fortipresence-rogue | Enable/disable FortiPresence reporting of Rogue APs |
| fortipresence-unassoc | Enable/disable FortiPresence reporting of unassociated devices |
| fortipresence-source | Where UDP packets are sent from: the FortiAP, the Controller, or both |

In this example,

```
edit "FAP-223-Sensor"
      config platform
         set type 223B
      end
   set ap-country US
      config radio-1
         set band 802.11n-5G
         set vaps "SocialWiFi"
         set channel "36" "48" "149" "157" "165"
      end
      config radio-2
         set band 802.11n
         set vaps "SocialWiFi"
         set channel "1" "6" "11"
      end
      config lbs
         set station-locate enable
         set fortipresence enable
         set fortipresence-server
```

```
            set fortipresence-port
            set fortipresence-secret
            set fortipresence-project
            set fortipresence-frequency
            set fortipresence-rogue
            set fortipresence-source
        end
    next
```

Set the IP address, port and key to be used for the data feed. The IP address is the address of the location server. The port is the port used for communication between the controller and the location server. The key should match the value set on the location server. It is used to sign the packets to ensure their validity. The update frequency specifies how frequently updates should be sent for a client and is measured in seconds. The default is 30 seconds. With a 30 second default, the AP will send an update every second with 1/30th of the client devices. The client devices will be spread out across the 30 seconds based on MAC address. There will be an update every 30 seconds for each client. Increasing the frequency can have a negative impact on location data in congested wireless networks. The includeUnassocSta flag will cause the unassociated client device data to be included in the feed. In this case, unassociated clients mean devices that are not associated to any AP.

Please note that the traffic will be sent by UDP.

**Fortinet Implementation notes:**

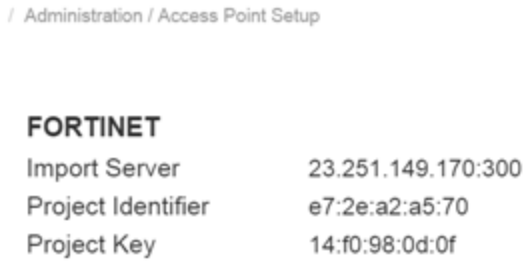
The sta-reports must still be sent out if no SSID is configured in the system.

1. Configure unit in monitor mode and also select a channel.
2. AP must not boradcast packets on any channel.
3. AP must listen on a single configured channel to collect all probe requests.
4. AP must not leave the channel, unless rogue AP scan is enabled.

**Message types:**

1. FortiAP identification
2. Station-locate datagram

**Display of Project Identifier and Secret in FortiPresence**




Project Identifier and Key are strings with maximally 16 ASCII characters. The Project Identifier indicate to which customer project the packets belong. The Project Key is a shared secret to sign each packet to in order to validate its authenticity and integrity.

# Configuring FortiPresence

The FortiPresence API extends the wireless retail analytics solution to retailers who can use data from the analytics report to understand customer behavior, for example when they arrive, length of stay or come into the store, how long they stay, and if they are a new or repeat customer.

The FortiPresence API is only supported on 802.11ac APs, and is only supported on SD version 8.1+.

When the location server feature is enabled on the controller, all 11ac APs send STA reports of STA/AP in their discovered list and STA in the assigned list at configured time intervals.

The controller forwards the STA reports to the data analytics server which then analyzes the data and provides user-friendly information to the user.

## Configuring the Controller

There are two report formats - **Legacy** and **FortiPresence**. The standard FortiPresence feed should be used by 3rd party partners. The information needed below can be obtained when you purchase a FortiPresence license for this feature.

The location-server feature can be enabled on the controller using the steps below.

The `location-server`, `project-name`, and `secret` entries shown below should match the **Import Server**, **Project Identifier**, and **Project Key** (respectively) found on the **Access Point Setup** page on the FortiPresence Insight WebApps portal.

1. Specify the location server IP address:
   ```
   config location-server ip-address 23.251.149.170:300
   ```
2. Specify the location server port. This port is used for communication between the controller and the location server:
   ```
   config location-server port 300
   ```
3. Specify the project name. The project-name indicates to which customer project the packets belong. Maximum of 16 ASCII characters can be used:
   ```
   config location-server project-name 81:95:fc:45:37
   ```
4. Specify a password, a pre-shared secret to sign each packet to in order to validate its authenticity and integrity. A maximum of 16 ASCII characters can be used:
   ```
   config location-server secret 0d:f3:14:1d:b7
   ```
5. Specify the report format. The standard FortiPresence feed should be used. A maximum of 16 ASCII characters can be used:
   ```
   config location-server report-format forti-presence
   ```
6. Specify an interval at which the location reports are queried (in seconds). The default is **5** seconds (a higher interval, such as **30** seconds, is recommended):
   ```
   config location-server report interval 30
   ```
7. Specify the location server source:

```
config location-server source wifi
```

To view the configuration, use the `show location-server` command:

```
show location-server
Location Server Configuration
ReportFormat                          : forti-presence
Project Name                          : FortiStore
Enable/Disable Location Server        : enable
Secret                                : *****
Location Server Source                : wifi
Location Server IP Address            : 1.1.1.1
Location Server Port                  : 300
Location Report Interval (in Seconds) : 30
```

The output indicates that all APs should send station-locate reports every 30 seconds and the controller forwards it to the server 1:1:1:1 configured on UDP port 300.

The update frequency specifies the frequency at which the updates are sent for a client and is measured in seconds. The default is 5 seconds.The client devices will be spread out across the 5 seconds based on MAC address. There will be an update every 5 seconds for each client. Note that increasing the frequency can have a negative impact on location data in congested wireless networks. The traffic will be sent as UDP.

## FortiWLC (SD) Communication ports

The following ports are used for communication between an AP and a controller:

| Traffic | Port |
|---|---|
| AeroScout | UDP/6091 |
| Captive Portal (HTTP redirection) | TCP/8080 |
| Captive Portal (HTTPS redirection) | TCP/8081 |
| NM Location Manager - Web UI | TCP/443 |
| NM Location Manager - Administrative Web UI (SSL) | TCP/8003 |
| NM Location Manager - AP Communication (Capture Packets subsystem) | UDP/9177and UDP/ 37008 |
| FTP | TCP/20 and TCP/21 |
| H.323v1 flow detection | TCP/1720 |
| HTTP | TCP/8080 |
| HTTPS | TCP/443 |
| Fortinet L3 AP COMM | UDP/5000 |

| Traffic | Port |
|---|---|
| Licensing - for connections initiated from within the controller only for licensing purposes (e.g. wncagent > merud) | TCP/32780 |
| Fortinet L3 AP Data | UDP/9393 |
| Fortinet L3 AP Discovery/Keepalive | UDP/9292 |
| NP1 advertisements / config | UDP/9980 |
| NTP | UDP/123 |
| RADIUS accounting | 1813 / 1646 |
| RADIUS auth | 1812 / 1645 |
| SIP | UDP/TCP 5060 |
| SSH | TCP/22 |
| SNMP | UDP/161 and 162 |
| Syslog | UDP/514 |
| TFTP | UDP/69 |
| UDP broadcast up to five upstream/downstream configurable | UPD/xxx |
| TACACS+ | TCP/49 |
| Telnet | TCP/23 |
| Controller packet capture | UDP/9177 |
| WIPS | UDP/9178 |
| WireShark, OmniPeek, Newbury | UDP/9177 |
| SAM (AP and server) | EtherIP 97 |

# FortiAP identification datagram packet format

The FAP identification datagram packet is sent out once an hour, or on every controller or FAP update. If no identification packets are received for longer than 10 update intervals the unit will be marked as “disconnected".

## Types of identification packets

The following are different identification packets.

### Controller

Controller identification packet
FAP1 identification packet
FAP2 identification packet
…
Signature

Limit the total bytes to 1500 to be lower than the MTU of the Ethernet. When running into this limit please use the following format.

*Alternatively*

Controller identification packet
FAP1 identification packet
…
Signature

Controller identification packet
FAP23 identification packet
…
Signature

### FAP

FAP identification packet
Signature

## Detailed packet structure

When sourced from Controller this header is pre-pended.

| Field Name | Bytes | Description | Default/Typical Value | Notes |
|---|---|---|---|---|
| Message type | 8 | String | "CTRL_ID_" | Identifies this message as originated from controller. It is a constant value. |
| Version of Push API | 2 | U (16) | 98 | Version number of the PushAPI protocol. “96” identifies v0.96. |
| Controller serial # | 18 | String | Example: "FGT60D3X13000846" | Must be filled to support debugging of communication problems. If no serial number available please use the base mac address. |
| Controller name | 24 | String | Example: "FortiGate-Store3334" | Blank if N/A |

| Field Name | Bytes | Description | Default/Typical Value | Notes |
|---|---|---|---|---|
| Controller OS version | 26 | String | Example: "FortiOS-v5.4.0-build364" | Controller OS version |
| VDOM name | 18 * | String | “Production-PCI” | Blank if N/A |

* - 96 bytes total

When sourced from FAP the packets look as below.

| Field Name | Byte-s | Descrip-tion | Default/Typical Value | Notes |
|---|---|---|---|---|
| Message type | 8 | String | "FAP_ID_" | |
| Version of Push API | 2 | U (16) | 98 | Version number of the PushAPI protocol. “96” identifies v0.96. |
| Project name | 16 | String | "Project-Exonn" | As given from Fortinet CLI |
| Sequence # | 2 | U (16) | Starts at 0 up to 65536 and wraps | Sequence number - running count of message from this sensor. Wraps around. This message is sent out once an hour or every time configuration changes. |
| Major version | 1 | U (8) | | Set to 4 |
| Minor version | 1 | U (8) | | Set to 0 |
| AP Boar d_MAC1 | 6 | | | AP MAC. Unique identifier for an AP |
| AP Boar d_MAC2 | 6 | | | |
| AP Radio 1 MAC | 6 | | | |
| Sta-locate-enabled | 1 | U (8) | | 0=no 1=yes |

| Field Name | Byte-s | Descrip-tion | Default/Typical Value | Notes |
|---|---|---|---|---|
| AP Radio 2 MAC | 6 | | | |
| Sta-locate-enabled | 1 | U (8) | | 0=no 1=yes |
| AP radio 3 MAC | 6 | | | |
| Sta-locate-enabled | 1 | U (8) | | 0=no 1=yes |
| AP Serial # | 18 | String | Example: "FAP14C3X13000846" | |
| AP Name | 64 | String | | |
| local_ ipv4_addr | 4 | UInt8[4] | | Array of unsigned 8 bit integers. |
| FAP OS version | 32 | String | Example: "FAP14C-v5.0-build064" | |
| connectio n_state (status) | 1 | U (8) | ideally always in connected state | 0= searching for controller 1= sulking 2= unauthorized 3= connected |
| Flags | 1 | | Binary bit flag Bit 1 = reports are encrypted Bit 2 = FAP has NTP sync | 0=No 1=yes e.g: 2 = NTP sync, not encrypted |
| Reserved | 1 | | | |
| Signature | 20 | | HMAC-SHA1 Signature Example: 77afea82bb987295e533d6acedf425c05d2850e5 | http://www.freeformatter.com/hmac-generator.html#ad-output |

# Station-locate datagram packet format

The following are different identification packets.

## Controller

Controller identification packet
FAP1 station report header packet
Station report 1 packet

Station report 2 packet
…
FAP2 station report header packet
Station report 1 packet
Station report 2 packet

…
Signature

Limit the total bytes to 1280 to be lower than the MTU of the Ethernet. When running into this limit please use the following format.

*Alternatively*

Controller station report header packet
FAP1 station report header packet
Station report 1 packet
Station report 2 packet
…
Siganture

Controller station report header packet
FAP2 station report packet
Station report 1 packet
Station report 2 packet
…
Signature

### FAP

FAP station report header packet
Station report 1 packet
Station report 2 packet
…
Signature

Limit the total bytes to 1280 to be lower than the MTU of the Ethernet. When running into this limit please use the following format.

*Alternatively*

Split the following packet into packets each with less than 1280 bytes.

FAP station report header packet
Station report 1 packet
Station report 2 packet
…
Station report 100 packet
Station report 101 packet
…
Signature

The two station locate reports are shown below:

FAP station report header packet
Station report 1 packet

Station report 2 packet
…
Signature

FAP station report header packet
Station report 100 packet
Station report 101 packet
…
Signature

| ip | udp | sta_locate_hdr | sta_locate_payload | Sta_locate_signature |

## Sta-locate Header

When sourced from Controller this header is pre-pended.

| Field Name | Bytes | Description | Default/Typical Value | Notes |
|---|---|---|---|---|
| Message type | 8 | String | "CTRL_STA" | Identifies this message as originated from Controller and a project Identification packet. |
| Version of Push API | 2 | U (16) | 98 | Version number of the PushAPI protocol. “96” identifies v0.96. |
| Controller serial # | 18 * | String | Example: "FGT60D3X13000846" | Must be filled |

* - 28 bytes total

When sourced from FAP the packets look as below.

| Field Name | Bytes | Description | Default/Typical Value | Notes |
|---|---|---|---|---|
| Message type | 8 | String in ASCII | "FAP_STA" | Fortinet Station report |
| Version of Push API | 2 | U (16) | 98 | Version number of the PushAPI protocol. “96” identifies v0.96. |
| Sequence # | 2 | Sequence number - running count of message from this sensor. Wraps around | | start at 0 |

| Field Name | Bytes | Description | Default/Typical Value | Notes |
|---|---|---|---|---|
| # of Messages | 1 | # of sta-locate messages in this payload | 1 to 40 typical values | |
| FAP Serial # | 18 | Serial # of FAP | FP223B3X14000589 | |
| AP MAC | 6 | AP Base MAC. Unique identifier for an AP. | Example: 085b0e8813b6 | Normally the copper Ethernet address |
| Padding | 2 * | | | |

* - 39 bytes total

## Sta_locate_Signature

A 20 byte signature is included at the end of every message. This is a HMAC-SHA1 signature created by using the shared secret as the key and the contents of RTLS packet as the data.

| Sta_locate_report Field (http://www.-freeformatter.com/hmac-gen-erator.html#ad-output) | Byte-s | Description | Notes |
|---|---|---|---|
| Radio_BSSID (sn) | 6 | BSSID of the radio that detected the device | APradioMacAddressSense that sensed the client |
| MAC (or si) | 6 | MAC address of station/device/phon e | e.g. iPhone mac address |
| BSSID (or bi) | 6 | BSSID with which this station is associated | APradioMacAddressAssociated to which the station is associated |
| Type (or ap) | 1 | Type of device | 0 = Wireless CLIENT<br>1 = Wireless AP (potential rogue) |

| Sta_locate_report Field (http://www.-freeformatter.com/hmac-gen-erator.html#ad-output) | Byte-s | Description | Notes |
|---|---|---|---|
| Data rate | 1 | Data rate of last transmission | Set to 0XFF for unassociated stations:<br>1 = 0x00<br>2 = 0x01<br>5.5 = 0x02<br>6 = 0x03<br>9 = 0x04<br>11 = 0x05<br>12 = 0x06<br>18 = 0x07<br>24 = 0x08<br>36 = 0x09<br>48 = 0x0A<br>54 = 0x0B<br>>54 = 0x0C |
| Channel | 1 | Channel where this station is active | |
| Avg Signal (avg RSSI) | 1 | Average Signal level dBm. | Signal strength is decimal between 128 to -128. Typically between -30 to -95 dBm reported |
| Num_packets | 2 | Number of packets used in average RSSI calculation | |
| Min Signal | 1 | Minimum Signal Strength in this period | Signal strength is decimal between 128 to -128. Typically between -30 to -95 dBm reported. If not available use average RSSI. |
| Max Signal | 1 | Max Signal Strength in this period | Signal strength is decimal between 128 to -128. Typically between -30 to -95 dBm reported. If not available use average RSSI. |

| Sta_locate_report Field (http://www.-freeformatter.com/hmac-gen-erator.html#ad-output) | Byte-s | Description | Notes |
|---|---|---|---|
| Age of First observation | 4 | Age of first observation in 1/100's of sec | Example: 1234 1234/100 = 12.34 seconds The first observation was 12.34 seconds before the UDP packet is sent out. Receiver will use its own time stamp for actual time.<br>Note that age is being used instead of a timestamp to avoid issues with unsynchronized system clocks. |
| Age of Last observation | 4 | Age of last observation in 1/100's of sec | Example: 1000 1000/100 = 10 seconds The last observation was 10 seconds before the UDP packet is sent out. Receiver will use its own time stamp for actual time. |
| X | 2 | 2D location of client as calculated by location engine. Value X | 0,0 is origin at bottom left X=0X8000, is bottom right 0xFFFF means invalid See note below for example |
| Y | 2 | 2D location of client as calculated by location engine. Value Y | 0,0 is origin at bottom left Y=0X8000, is top left 0xFFFF means invalid. See note below for example |
| Reserved | 2 | reserved | |
| Signature | 20 | HMAC-SHA1 Signature | http://www.freeformatter.com/hmac-generator.html#ad-output |

Total bytes with Signature = 60
Total bytes Sta_locate_report = 40
Totel bytes message with header and signature = 127

**Note:** The X,Y data is scaled to always be between 0x0 and 0x8000 independent of actual size of venue.

| | |
|---|---|
| 0x0, 0x8000 | 0x8000,0x8000 |
| | |
| | |
| | |
| 0x0,0x0 | 0x8000,0x0 |

## Compound Message Report

The UDP must contain multiple updates for efficient bandwidth use. Please pack up to 40 updates in a single datagram. Please re-compute this by configured MTU.

This would be:

| | |
|---|---|
| Header | 40 bytes |
| Sta-locate-report | 40 bytes |
| Sta-locate-report | 40 bytes |
| Sta-locate-report | 40 bytes |
| Sta-locate-report | 40 bytes |
| Sta-locate-report | 40 bytes |
| Sta_locate_signature | 20 bytes |

Messages from 36 client MAC addresses can be compacted into a single UDP datagram 40B Header + (36 x 40 bytes sta-locate) + 20 Byte signature = 1456 byte UDP payload.

# General Questions

The following section addresses some general questions.

## How frequently are updates sent?

The update interval sets how often updated information for a single device will be sent in the sta-locate data stream. If it is set to 30 seconds, sta-locate data for a specific clients that were observed in that time period will be sent every 30 seconds.

## RogueAP-locate datagram packet format

| ip | udp | sta_locate_hdr | sta_locate_payload | Sta_locate_signature |

### RogueAP-locate Header

When sourced from Controller this header is pre-pended.

| Field Name | Bytes | Description/Default | Default/Typical Value | Notes |
|---|---|---|---|---|
| Message type | 8 | String in ASCII | "CTRL_ROG" | Identifies this message as originated from Controller and a project Identification packet |
| Version of Push API | 2 | U (16) | 98 | Version number of the PushAPI protocol. “96” identifies v0.96. |
| Controller Serial # | 16 | String | Example: "FGT60D3X13000846" | Must be filled |

When sourced from FAP the packets look as below:

| Field Name | Bytes | Description/Default | Default/Typical Value | Notes |
|---|---|---|---|---|
| Message type | 8 | Configure with "FAP_RGAP" | "FAP_RGAP" | Fortinet Rogue AP report |
| Version of Push API | 2 | U (16) | 97 | Version number of the PushAPI protocol. “96” identifies v0.96. |

| Field Name | Bytes | Description/Default | Default/Typical Value | Notes |
|---|---|---|---|---|
| Sequence # | 2 | Sequence number - running count of message from this sensor. Wraps around | | start at 0 |
| # of Messages | 1 | # of sta-locate messages in this payload | 1 to 40 typical values | |
| FAP Serial # | 16 | Serial # of FAP | FP223B3X14000589 | |
| AP MAC | 6 | AP Base MAC. Unique identifier for an AP. | Example: 085b0e8813b6 | Normally the copper Ethernet address |
| Padding | 2 * | | | |

* - 36 bytes total

## Rogue_AP_locate_Signature

A 20 byte signature is included at the end of every message. This is a HMAC-SHA1 signature created by using the shared secret as the key and the contents of RTLS packet as the data.
http://www.freeformatter.com/hmac-generator.html#ad-output

## Rogue_AP_locate_report

| Field | Bytes | Description | Notes |
|---|---|---|---|
| Radio_BSSID (sn) | 6 | BSSID of the radio that detected the device | |
| MAC (or si) | 6 | MAC address of station | |
| BSSID (or bi) | 6 | BSSID with which this station is associated | |

| Field | Bytes | Description | Notes |
|---|---|---|---|
| Type (or ap) | 1 | Type of device | 0 = Wireless CLIENT<br>1 = Wireless AP (potential rogue)<br>(is always 1 for Rogue report) |
| Data rate | 1 | Data rate of last transmission | Set to 0 for unassociated stations:<br>1 = 0x00<br>2 = 0x01<br>5.5 = 0x02<br>6 = 0x03<br>9 = 0x04<br>11 = 0x05<br>12 = 0x06<br>18 = 0x07<br>24 = 0x08<br>36 = 0x09<br>48 = 0x0A<br>54 = 0x0B<br>>54 = 0x0C |
| Channel | 1 | Channel where this station is active | |
| Avg Signal (avg RSSI) | 1 | Average RSSI during the duration. RSSI is signal strength. Signal is a signed negative hex value. | Signal strength is decimal between 128 to -128. Typically between -30 to -95 dBm reported. Convert Hex to decimal and subtract 256 to get the signal value. |
| Num_packets | 2 | Number of packets used in average RSSI calculation | |

| Field | Bytes | Description | Notes |
|---|---|---|---|
| Min RSSI | 1 | Minimum Signal Strength in this period | Signal strength is decimal between 128 to -128. Typically between -30 to -95 dBm reported. Convert Hex to decimal and subtract 256 to get the signal value. |
| Max RSSI | 1 | Max Signal Strength in this period | Signal strength is decimal between 128 to -128. Typically between -30 to -95 dBm reported. Convert Hex to decimal and subtract 256 to get the signal value. |
| Age of First observation | 4 | Age of first observation in 1/100's of sec | Example: 1234 1234/100 = 12.34 seconds The first observation was 12.34 seconds before the UDP packet is sent out. Receiver will use its own time stamp for actual time. |
| Age of Last observation | 4 | Age of last observation in 1/100's of sec | Example: 1000 1000/100 = 10 seconds The last observation was 10 seconds before the UDP packet is sent out. Receiver will use its own time stamp for actual time. |
| X | 2 | 2D location of client as calculated by location engine. Value X | 0,0 is origin at bottom left X=0X8000, is bottom right 0xFFFF means invalid See note below for example. |
| Y | 2 | 2D location of client as calculated by location engine. Value Y | 0,0 is origin at bottom left Y=0X8000, is top left 0xFFFF means invalid. See note below for example. |
| SSID | 33 | Name of SSID | Full SSID of the Rogue AP up to 33 characters. |
| Reserved | 1 | reserved | |
| Signature | 20 | HMAC-SHA1 Signature | http://www.freeformatter.com/hmac-generator.html#ad-output |

Total bytes with Signature = 92
Total bytes Rogue_AP_locate_report = 72
Total bytes message with header and signature = 128

## Compound Message Report

The UDP must contain multiple updates for efficient bandwidth use. Please pack up to 40 updates in a single datagram. Please re-compute this by configured MTU.

This would be

| | |
|---|---|
| Header | 36 bytes |
| Rogue_AP_locate_report | 72 bytes |
| Rogue_AP_locate_report | 72 bytes |
| Rogue_AP_locate_report | 72 bytes |
| Rogue_AP_locate_report | 72 bytes |
| Rogue_AP_locate_report | 72 bytes |
| Sta_locate_signature | 20 bytes |

Messages from 20 RogueAP BSSID and SSIDs can be compacted into a single UDP datagram 36B Header + (20 x 72 bytes sta-locate) + 20 Byte signature = 1496 byte UDP payload.