FORTINET
High Performance Network Security

FortiPresence

Push API Reference Guide

Version 0.100

Contents

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

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

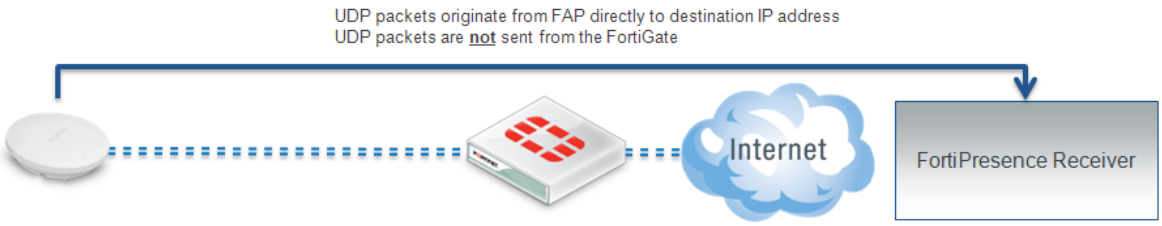
Change Log

Date	Change Description
2020-10-21	• Added the Association status field to sta_locate signature. • Push API version updated to 100.
2020-12-01	Updated the sta-locate-re value to 41.
2020-02-01	Updated some field descriptions and bytes.

Overview

The following document defines the APIs for presence analytics messages to be posted to services such as FortiPresence or 3rd party. This API allows each FAP access point to forward station update messages directly to presence analytics collector without the need to go thru the FortiGate controller or FortiCloud.

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 Controller as well.



The document contains fields that are common to both infrastructure APs and FAP-U APs.

Pull API vs 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.

Configuring FortiGate

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.

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

```
    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
# The following highlighted commands are meant for FortiPresence team.
              set fortipresence enable
              set fortipresence-server   [enter server IP or DNS name]
              set fortipresence-port     [enter UDP port: default 300]
              set fortipresence-secret   [enter up to 16 characters]
              set fortipresence-project  [enter up to 16 characters]
              set fortipresence-frequency[reports sent every x seconds,
default 30 seconds]
              set fortipresence-rogue enable [also send Rogue AP report]
              set fortipresence-source FAP, Controller, Both [ Selects
where UDP packets are sent from]

            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.

Note: The traffic will be sent UDP

Implementation Guidelines

The station 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 broadcast packets on any channel
3. AP must listen on a single configured channel to collect all probe requests.

AP must not leave the channel, unless rogue AP scan is enabled.

The following message types are supported:

- FortiAP identification
- 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 indicates 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.

Identification datagram packet format

• 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

Controller
Controller identification packet
FAP1 identification packet -- One controller see multiple FAPs
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 -- One controller see multiple FAPs
….
Signature
Controller identification packet
FAP23 identification packet
….
Signature

FortiAP Identification Packet

Signature
Detailed packet structure
When sourced from Controller this header is pre-pended

Field Name	Bytes	Type	Default/typical Value	Notes
Message Type	8	String	"CTRL_ID_"	Identifies this message as originated from controller. It is a constant value.
Version of PushAPI	2	U(16)	100	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
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 FortiAP the packets look as below.

Field Name	Bytes	Type	Default/typical Value	Notes
Message Type	8	String	"FAP_ID__"	Identifies this message as originated from controller. It

				is a constant value.
Version of PushAPI	2	U(16)	100	Version number of the PushAPI protocol. “96” identifies v0.96.
Projectname	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 7	
Minor version	1	U(8)	Set to 1	
AP Board_MAC1	6			AP MAC. Unique identifier for an AP
AP Board_MAC2	6			
AP Radio1 MAC	6			
Tx Power Radio-1	1	U(8)		EIRP value
Sta-locate-enabled	1	U(8)		0=no 1=yes
AP Radio 2 MAC	6			
Tx Power Radio-2	1	U(8)		EIRP value
Sta-locate-enabled	1	U(8)		0=no 1=yes
AP radio 3 MAC	6			
Tx Power Radio-3	1	U(8)		EIRP value
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"	
connection_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	32		SHA256 Signature Example: 77afea82bb987295e533d6acedf425c05d2850e5	https://www.freeformatter.com/sha256-generator.html

Station-locate datagram packet format

Controller

Controller station report header packet
FAP1 station report header packet -- One controller see multiple FAPs
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 -- One controller see multiple FAPs
Station report 1 packet
Station report 2 packet
….

Signature

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	Type	Default/typical Value	Notes
Message Type	8	String	"CTRL_STA"	Identifies this message as originated from Controller and a project Identification packet.
Version of PushAPI	2	U(16)	100	Version number of the PushAPI protocol. “96” identifies v0.96.
Controller Serial #	18	String	Example: "FGT60D3X13000846"	Must be filled

Total = 28 bytes

When sourced from FAP the packets look as below.

Field Name	Bytes	Type	Default/typical Value	Notes
Message Type	8	String in ASCII	FAP_STA_	Fortinet Station report
Version of PushAPI	2	U(16)	100	Version number of the PushAPI protocol. “96” identifies v0.96.
Sequence #	2		start at 0	Sequence number - running count of message from this sensor. Wraps around
# of Messages	1		1 to 34 typical values	# of sta-locate messages in this payload
FAP Serial #	18		FP223B3X14000589	Serial # of FAP
AP MAC	6		Example: 085b0e8813b6	AP Base MAC. Unique identifier for an AP. Normally the copper Ethernet address

Padding	2			

Sta_locate_ Signature

A 32 byte signature is included at the end of every message. This is a SHA256 signature created by using the shared secret as the key and the contents of RTLS packet as the data. https://www.freeformatter.com/sha256-generator.html

Field Name	Bytes	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/phone	e.g. iPhone mac address
BSSID (or bi)	6	BSSID with which this station is associated	For device type 0 & 1: APradioMacAddressAssociated to which the station is associated Type 2: 0 (zero)
Association status	1	Indicates if the MAC is associated to the reporting AP.	0=APradioMacAddressAssociated to which the station is associated is NOT from AP's BSSID list. 1=APradioMacAddressAssociated to which the station is associated is from AP's BSSID list.
Type (or ap)	1	Type of device	0 = wireless CLIENT, 1 = Wireless AP (potential rogue) 2 = BLE
Data rate	1	Data rate of last transmission	Set to 0XFF for unassociated stations Values 1 = 0x00 2 = 0x01 5.5 = 0x02 6 = 0x03 9 = 0x04

			11 = 0x05 12 = 0x06 18 = 0x07 24 = 0x08 36 = 0x09 48 = 0x0A 54 = 0x0B >54 = 0x0C
Channel	1	Channel where this station is active	Device type 2->0
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.
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 is being used instead of a timestamp to avoid issues with unsynchronized system clocks.) (NOTE: Device Type 2 should be zero)
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. (NOTE: Device Type 2 should be zero)
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 (NOTE: Device Type 2 should be zero)
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 (NOTE: Device Type 2 should be zero)
Reserved	2	reserved	
Signature	32	SHA256 Signature	https://www.freeformatter.com/sha256-generator.html
Total Bytes with Signature	73		
Total Bytes Sta_locate_report	41		
Total Bytes Message with header and signature	140		

Note on location: 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 34 updates in a single datagram. Please re-compute this by configured MTU.

Field Name	Bytes
Header	40 bytes
Sta-locate-report	41 bytes
Sta-locate-report	41 bytes
Sta-locate-report	41 bytes
Sta-locate-report	41 bytes
Sta-locate-report	41 bytes
Sta_locate_signature	32 Bytes

Messages from 34 client MAC addresses can be compacted into a single UDP datagram 40B Header + (34 x 41 bytes sta-locate) + 32 Byte signature = 1466 byte UDP payload.

FAQs

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 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		Default/typical Value	Notes
Message Type	8	String	"CTRL_ROG"	Identifies this message as originated from Controller and a project Identification packet
Version of PushAPI	2	U(16)	100	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	Possible Values	Notes
Message Type	8	Configure with "FAP_RGAP"	FAP_RGAP	Fortinet Rogue AP report
Version of PushAPI	2	U(16)	100	Version number of the PushAPI protocol. “96” identifies v0.96.
Sequence #	2	Sequence number - running		start at 0

		count of message from this sensor. Wraps around		
# of Messages	1	# of sta-locate messages in this payload	1 to 19 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			

Total length 36 bytes

Rogue_AP_locate_ Signature

A 32 byte signature is included at the end of every message. This is a SHA256 signature created by using the shared secret as the key and the contents of RTLS packet as the data. https://www.freeformatter.com/sha256-generator.html

Rogue_AP_locate_report

Field Name	Bytes	Description	Notes
Radio_BSSID	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	
Type (or ap)	1	Type of device	0 = wireless CLIENT, 1 = Wireless AP (potential rogue)

			(is always 1 for Rogue report)
Data rate	1	Data rate of last transmission	Set to 0 for unassociated stations. Values 1 = 0x00 2 = 0x01 5.5 = 0x02 6 = 0x03 9 = 0x04 11 = 0x05 12 = 0x06 18 = 0x07 24 = 0x08 36 = 0x09 48 = 0x0A 54 = 0x0B >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	
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	32	SHA256 Signature	https://www.freeformatter.com/sha256-generator.html
Total Bytes with Signature	104		
Total Bytes Rogue_AP_locate_report	72		
Total Bytes Message with header and signature	140		

Compound Message Report

The UDP must contain multiple updates for efficient bandwidth use. Please pack up to 19 updates in a single datagram. Please re-compute this by configured MTU.
This would be

Field Name	Bytes
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
Rogue_AP_locate_ Signature	32 Bytes

Messages from 19 RogueAP BSSID and SSIDs can be compacted into a single UDP datagram

36B Header + (19 x 72 bytes sta-locate) + 32 Byte signature = 1436 byte UDP payload