

Gateway Cloud API

The information below is a swagger definition for the SensorPush public API for the Gateway cloud. Download the swagger definition file here.

Note that requests can be made no more than once per minute. If you need support, please reach out to support@sensorpush.com, please be sure to preface your email subject with "[api]" so it reaches the correct team.

Important! To activate your API access, please log in to the Gateway Cloud Dashboard and agree to the terms of service. Once you've logged in that initial time, your account will have access. You can review the terms here.

```
        Base URL:
        https://api.sensorpush.com/api/v1

        Version:
        v1.0.20250413

        Schemes:
        https://api.sensorpush.com/api/v1
```

Examples

The following illustrates how to interact with the API via simple curl commands.

Important FYI about tokens

The authorization token is returned after a successful signin. This token identifies the user as a trusted client, and is valid for 60 minutes.

The authorization token is used to request two additional tokens: access and refresh tokens. The access token authorizes the user to begin using the API. This token is valid for 3D minutes, at which time the client must request a new access token using the refresh token.

The refresh token is valid for 60 minutes. Upon requesting a new access token, the client will receive new refresh token as well. The access token is valid for another 30 minutes, and the refresh token is again valid up to an additional 60 minutes.

These steps are in accordance with the oAuth2 specifications such that if any of the three tokens are lost, the tokens eventually expire, thus securing the account once again.

For additional information, please refer to the oAuth website

Important FYI about Gateways:

A Gateway steadily relays sensor data roughly every minute. In addition to that, a Gateway will periodically check in with the cloud to make a record to indicate that that Gateway is on and connected to the Sensor/Fush cloud via the Internet. A Gateway's check in can be observed by reading the "last_seen" property of a Gateway Consider evaluating the "last_seen" property of a Gateway roughly every 15 minutes for a reliable indication of its status.

Example 1 - Step 1: Authorization

Log in using a valid email/password to recieve an authorization code.

```
copy to diplomed

surd x 80° integration integration confequency described authorize "\
""> corpy: application/jees"\
""> application/jees"\
""> application/jees"\
""> application/jees"\
""> application/jees"\
""> application/jees"\
""> application/jees\
""> application/jee
```

Example 1 - Step 2: OAuth Access

Request a temporary oauth access token. Use the result from the previous step for the authorization code in the body.

```
copy to diploand

cord. 1 Post 'nttps://gi.sensorpush.com/gi/vi/oantNuccesstaken' \
"Scopt: application/joon' \
"Cartherization" 'carthorization'
"Scopt: application/joon' \
"Carthorization' 'carthorization'
```

Example 2: List Gateway

Request a list of gateways. Add the header "Authorization: " using the accesstoken returned in the OAuth Access step

Example 3: List Sensors

Request a list of sensors. Add the header "Authorization: " using the accesstoken returned in the OAuth Access step.

Example 4: Query Samples

Request up to 20 samples occuring after a timestamp with this format YYYY-MM-DDThh:mm:ss.0002, and also add the header "Authorization:" using the accesstoken returned in the OAuth Access step.

Data for temperature is in Fahrenheit.

```
copy to diplocad

card 3 of "stages//pmi demonrpash.com/api/vi/samples" \
ii "scopt: application/joan"
ii "claim": 20 )
acor
```

${\it Example 5: Query Samples for Specific Sensors and/or Specific Start and Stop Times}$

Similar to the "Query Samples" example, but with an added array for specific sensor IDs, and also added startTime and stopTime.

Security

```
Oauth

Name:
Authorization

In:
Header
Description:
This header value grants temporary access to data resources. Use the accesstoken value returned by the accesstoken service.
```

7 Help

Paths

		Description
/	POST	SensorPush API status
/devices/gateways	POST	Lists all gateways.
/devices/sensors	POST	Lists all sensors.
/oauth/accesstoken	POST	Request a temporary oAuth access code.
/oauth/authorize	POST	Sign in and request an authorization code
/oauth/token	POST	oAuth 2.0 for authorization, access, and refresh tokens
/reports/download	POST	Download bulk reports.
/reports/list	POST	Lists reports available for download.
/samples	POST	Queries for sensor samples.
/tags	POST	Updates tags on devices.

Description:		
his service is used as a simple method for clie	nts to verify they can connect to the API.	
desponses:		
application/json		
00 response		
Status		
	Data type	
Status	Data type string	
Status Header		

escription: is service will return an inventory of all register	red gateways for this account.	
sponses:		
application/json		
00 response		
Gateways		
00 response		
Error		
Header	Data type	
Access-Control-Allow-Headers	string	
Access-Control-Allow-Methods	string	
Access-Control-Allow-Origin	string	
00 response		
Error		
Header	Data type	
Access-Control-Allow-Headers	string	
Access-Control-Allow-Methods	string	
Access-Control-Allow-Origin	string	
scurity:		

escription: his service will return an inventory of all register	and concour for this account	
esponses:	ad sensors for this account.	
application/json		
00 response		
Sensors		
00 response		
Error		
Header	Data type	
Access-Control-Allow-Headers	string	
Access-Control-Allow-Methods	string	
Access-Control-Allow-Origin	string	
00 response		
Error		
Header	Data type	
Access-Control-Allow-Headers	string	
Access-Control-Allow-Methods	string	
Access-Control-Allow-Origin	string	
ocurity:		

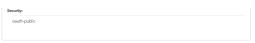
POST / auth/accestoken Request a temporary oAuth access code.
Description:
This is a simplified version of oAuth in that it only supports accesstokens and does not require a client_id. See the endpoint
'/api/v1/oauth/token' for the more advanced oAuth endpoint. Once a user has been authorized, the client app will call this
service to receive the access token. The access token will be used to grant permissions to data stores. An access token expires
every hour. After that, request a new access token.
Responses:
application/json
200 response
AccessTokenResponse

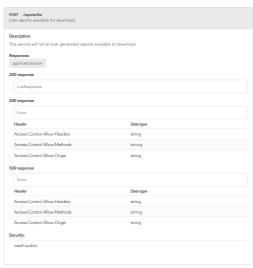
Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin	string
0 response	
Error	
Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin	string
0 response	
Error	
Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin	string

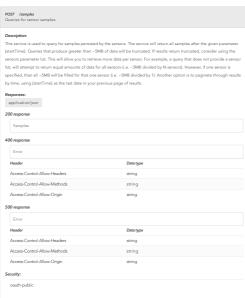
lescription:	rPush logon. Then signin using email/password, or an api id. This service
	changed for an oAuth access token using the accesstoken service.
esponses:	
application/json	
00 response	
AuthorizeResponse	
Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin 00 response Error	string
00 response	string Data type
00 response	
00 response Error Header	Data type
00 response Error Header Access-Control-Allow-Headers	Date type string
Error Header Access-Control-Allow-Headers Access-Control-Allow-Methods	Data type string string
00 response Erner Header Access Control-Allow-Headers Access Control-Allow-Mehods Access Control-Allow-Origin	Data type string string
00 response Error Header Access-Control-Allow-Headers Access-Control-Allow-Methods Access-Control-Allow-Origin	Data type string string
00 response Ernor Header Access Control-Allow-Headers Access Control-Allow-Methods Access Control-Allow-Origin valid user 00 response	Data type string string
00 response Error Meader Access Control-Allow-Headers Access Control-Allow-Methods Access Control-Allow-Origin walfol user 00 response Error	Data type string string string
00 response Error Header Access Control-All ow-Headers Access Control-All ow-Methods Access Control-All ow-Origin would user 00 response Error Header	Data type string string string

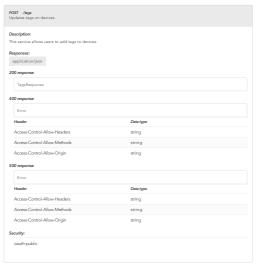
OST /oauth/token Auth 2.0 for authorization, access, and refresh tok	cens
	s the oAuth 2.0 specification. Supports grant_types: password, refereb, tok oken will be returned. (see oAuth Grant Types). A client_id is required for t gister your application and recieve a client_id.
00 response	
TokenResponse	
Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin	string
0 response Error Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin	string
00 response	
Error	
Header	Data type
Access-Control-Allow-Headers	string
Access-Control-Allow-Methods	string
Access-Control-Allow-Origin	string

POST /reports/download Download bulk reports.		
Description:		
This service will download bulk generated report	5.	
Responses:		
application/json		
200 response		
100 response		
Error		
Header	Data type	
Access-Control-Allow-Headers	string	
Access-Control-Allow-Methods	string	
Access-Control-Allow-Origin	string	
500 response		
Error		
Header	Data type	
Access-Control-Allow-Headers	string	
Access-Control-Allow-Methods	string	
Access-Control-Allow-Origin	string	









Schema definitions

AccessTokerMeguest
Types: object

Description:
Request object for an oAuth accesstoken code.

Proporties:
authorization: string

Authorization code received from the oauth/authorize service.

AccessTokenResponse Type: object

Description:
Request object for an oAuth authorize
Properties:
email: string
Email associated with a valid account Description:
Response object for an oAuth authorization code.
Properfies:
authorization: string
JWT oAuth authorization code. Pass this code to it
(https://yet.lo/) website has a useful jet viewer. Properties: message: string Gateway Type: object Properties: last_alert: string Date last alert was sent message: string Detailed message ass paired: string Gateway is paired tags: object List of tags assor Description:

Map of registered SensorPush gateways Description: Request object for gateways ListResponse Type: object Properties: files: array ReportListing Type: object Properties: last_modified: string Date file was last modified name: string Name of the file size: string File size ReportsRequest Type: object Description:
Request object for reports.
Properties:
path: string
The directory path to perfo Sample Type: object

Description:
This represents one observation recorded by a given sensor. The fields listed below (except for observed) will be populated base on the measures parameter specified in the request, and if the given sensor version collects that particular measure. For example, barometric_pressure is not available in HT1 series sensors, and thus will not be reported.

Properties: altitude: number Value unit is feet (ft)

barometric_pressure: number Value unit is inch of mercury (inHg)

humidity: number

Value unit is percentage (%)

temperature: number

Value unit is farenheit (°F)

Description:
Map of registered SensorPush sensors

Poperties:

last_time: string

ISO date time of the last sample returned. Use this as the start_ts to query for the next pa

sensors: object

Map of sensors and the associated samples.

total_samples: number Total number of samples across all

total_sensors: number Total number of sensors

truncated: boolean

Description: Request object for samples.

Properties:
active: boolean
Filters sensors by active = (true|false). Defaults to true.

Quelies that remi large results are truncated (see comments on Samples endpoind). Set this flag to true for large reports. The report request will be queued and processed within 24 hours. Upon completion, the primary account holder will recieve an email with a link for download.

limit: integer

Number of samples to return.

measures: array
Specifies which measures to include ("temperature" | "humidity" | "ypd" | "barometric_pressure" | "de measures are not available on older devices.

sensors: array

Filters samples by sensor id. This will be the sar strings. Example: sensors: (*123.56789*).

startTime: string
Start time to find samples (example: 2019-04-07700-00-00-0400). Leave blank or zero to get the most stopTime: string

Stop time to find samples (example: 2019-04-07T10:30.00-0400). Leave blank or zero to get the m

Properties:

active: boolean
Is the sensor active?

address: string MAC address

Properties: enabled: boolean Is enabled?

min: number Min threshold for alert

Properties: enabled: boolean Is enabled?

max: number Max threshold for alert

id: string Long device ld name: string
Name of the sensor sensor rssi: number Wireless signal strength in dB at last reading Sensors Type: object Description:
Request object for sensors.
Properties:
active: boolean
filters sensors by active – (tr Status Type: object Required:

message

Properties:
deployed: string

Date time when this message: string Greeting message stack: string
Active stack hosting this status: string Current status of the api se time: string
Current date time on the server **Tags** Type: object Description:
Map of registered devices and their tags. Properties: gateways: object sensors: object Description:
Map of registered devices and their tags.
Properties:
sensors: object TagsResponse Type: object Description:
Response object
Properties:
status: string
Message indicat

Message indicating if the tags were successfully updated.

| Description: | Descr

This can be an authorization, access, or refresh token. Depending on which grant_type you are using grant_sypes string
Accepted values are password, refresh_token, and access_token
passwords string
Her is password
readwact_unit string
Reciferation unit to the 3rd party application once the user has signed into the sensorpush logon. This value should be URL encoded.

refresh_token string
Reflected token used for request new access tokens.

username: string
Email of the user to sign in.

ToleroReporter

Description:

Response object for an oAuth authorization code.

Response object for an oAuth authorization code.

Reporter:

accest, token: string

JWT oAuth access token. Plass this token to the data services via the http header 'Authorization'. Example 'Authorization':

Bearer'

septing_Im number

TIT. of the token in seconds

refinesh_token: string

JWT oAuth refeels token. Plass this token to the token service to retrieve a new access token.

token_type: string

Type of token naturned

