

Setup

Generate Client Key

Send Event

Subscriptions

Received Messages

Random UUID

About



Remember keys. Note: Only use on a secure system. Stored as plain text at:
/var/folders/bv/7jtw7f1x5rlc4y8x03qf1jndgcy7bh/T//gambit/config.json

Copy Path

Secret Key

Access Key

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Remember keys. Note: Only use on a secure system. Stored as plain text at:
/var/folders/bv/7jtw7f1x5rlc4y8x03qf1jndgcy7bh/T//gambit/config.json

Copy Path

Secret Key

b8cdede1799ae7dbf63ce9682537fd7f636afb8eba6c01ca80bc0073169d44fcbdf8e630b2a15a663c6d3a413fef47a6

Access Key

6c4bc923b58ab45e6a04a06910de1f01

Setup

Generate Client Key

Send Event

Subscriptions

Received Messages

Random UUID

About

Generate Key

Client keys are secure keys that should be deployed with whatever apps you integrate Gambit with. Your main API secret key should remain completely secret and secure in your internal systems and should never be deployed into any client apps for security purposes due to app decompilation, and other methods which may give an attacker access to your primary secret key. Client keys are securely generated server-side by Gambit by requests against the `/client_secret` endpoint which requires your `secret_key` as the key to a HMAC-SHA256 hash over the JSON payload. The client keys consist of a `client_secret` and a `client_salt`. The `client_secret` is used as the HMAC key over the JSON payload to create the HMAC-SHA256 hash for authentication purposes to the `/event` endpoint. The `client_salt` is sent in the JSON payload as part of every event to Gambit. This combined with your `access_key` allows us to authenticate all `/event` calls to our system. This system allows you greater control over how you authorize devices, systems, or applications to hit our APIs. This design means that if a client key is compromised and is being abused, you can revoke access for certain `client_secret` / `client_salts` pairs without affecting other devices, apps, systems. This means that your primary `secret_key` stays secure and can continue to be used. If we did not have it setup this way, then you would have to revoke your main API key credentials which would affect all devices, apps, or systems that you used that API key as a basis for security / authentication.

Results

Client Salt

Client Secret

Raw Response

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Generate Key

Client keys are secure keys that should be deployed with whatever apps you integrate Gambit with. Your main API secret key should remain completely secret and secure in your internal systems and should never be deployed into any client apps for security purposes due to app decompilation, and other methods which may give an attacker access to your primary secret key. Client keys are securely generated server-side by Gambit by requests against the `/client_secret` endpoint which requires your `secret_key` as the key to a HMAC-SHA256 hash over the JSON payload. The client keys consist of a `client_secret` and a `client_salt`. The `client_secret` is used as the HMAC key over the JSON payload to create the HMAC-SHA256 hash for authentication purposes to the `/event` endpoint. The `client_salt` is sent in the JSON payload as part of every event to Gambit. This combined with your `access_key` allows us to authenticate all `/event` calls to our system. This system allows you greater control over how you authorize devices, systems, or applications to hit our APIs. This design means that if a client key is compromised and is being abused, you can revoke access for certain `client_secret` / `client_salts` pairs without affecting other devices, apps, systems. This means that your primary `secret_key` stays secure and can continue to be used. If we did not have it setup this way, then you would have to revoke your main API key credentials which would affect all devices, apps, or systems that you used that API key as a basis for security / authentication.

Results

Client Salt

Client Secret

Raw Response

```
{
  "client_secret": "eb64528c0d0c338d249af91c764fdd40468e7c93543ca72f7b06baf1384da880",
  "client_salt": "4bc57bdd8ae49eef4ed92f4abc0df400190c934d7b8c90128cda848bb7e9619e"
}
```

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Event Setup

Client Salt

Client Secret

Copy from generated keys

Namespace

Topic Description

New

Attribute Name	PK (Required)	Type	Value

Save

Namespace

Topic Description

Actions

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Event Setup

Client Salt Client Secret Namespace Topic Description

Attribute Name

PK (Required)

Type

Value

Namespace

Topic Description

Actions

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Event Setup

Client Salt 4bc57bdd8ae49eef4ed92f4abc0df40c

Client Secret eb64528c0d0c338d249af91c764fdd4

Copy from generated keys

Namespace Namespace_0317

Topic Description trael@aviatainc.com

New

Attribute Name	PK (Required)	Type	Value
email_address	<input checked="" type="checkbox"/>	Text	trael@aviatainc.com
cart_total	<input type="checkbox"/>	Integer	
club	<input type="checkbox"/>	Text	

Save

Namespace

Topic Description

Actions

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Event Setup

Client Salt Client Secret Namespace Topic Description

Attribute Name	PK (Required)	Type	Value

Namespace	Topic Description	Actions
Namespace_0317	trael@aviatainc.com	<input type="button" value="Delete"/>

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Event Setup

Client Salt	<input type="text" value="4bc57bdd8ae49eef4ed92f4abc"/>	Client Secret	<input type="text" value=":764fdd40468e7c93543ca72f7b06baf1384da880"/>	<input type="button" value="Copy from previous tab"/>
Timestamp	<input type="text"/>	<input type="text" value="?"/>	<input checked="" type="checkbox"/> Use current timestamp	
Namespace	<input type="text" value="Namespace_0317"/>	Debug Directive	<input type="text" value="echo-as-message"/>	<input type="text" value="?"/>
Event Name	<input type="text" value="Namespace_0317_echo_test"/>			

Attribute Name	PK (Required)	Type	Value
email_address	<input checked="" type="checkbox"/>	Text	trael@aviatainc.com
cart_total	<input type="checkbox"/>	Integer	6000
club	<input type="checkbox"/>	Text	
customer_id	<input type="checkbox"/>	Integer	
group	<input type="checkbox"/>	Text	emerald
login	<input type="checkbox"/>	Date	
page	<input type="checkbox"/>	Text	rings
product	<input type="checkbox"/>	Text	tiffany

```
On 2016-03-24 16:16:01 -0600:  
{"message": "request processed successfully"}
```

Setup

Generate Client Key

Subscriptions

Send Event

Received Messages

Random UUID

About

Clear

Date Received	Event Name	Topic Description	Campaign Name
Thu Mar 24 16:23:34 MDT 2016	Namespace_0317_echo_test	trael@aviatainc.com	NO-CAMPAIGN-FOR-ECHOED-EVENTS

Clear

Date Received	Event Name	Topic Description	Campaign Name
Thu Mar 24 16:23:34 MDT 2016	Namespace_0317_echo_test	trael@aviatainc.com	NO-CAMPAIGN-FOR-ECHOED-EVENTS

```
{
  "campaign_name": "NO-CAMPAIGN-FOR-ECHOED-EVENTS",
  "data":
  [{"access_key": "\6c4bc923b58ab45e6a04a06910de1f01", "debug_directive": "echo-as-message", "namespace": "Namespace_0317", "forw
    "namespace": "Namespace_0317",
    "event_name": "Namespace_0317_echo_test",
    "message_id": "0bbff970-f20f-11e5-95dd-f9b2417b80e4",
    "ciid_hash": "+2CYtII7ALI7bOvo3wV+l0pc5uCw+gPQtX7H0RCdVVI=",
    "campaign_id": -1
  }]
}
```