Authentication

Getting a key and secret

Before any calls can be made to the API, you must first have a key/secret pair that is used to authenticate your application. This key is associated with a set of permissions on a per server basis and the key/secret is only valid for that server.

> The key/secret pair is associated only with one server and that is the server it is created on

To get an key/secret, go to Virtual/Dedicated Server -> Sub accounts/API Keys and click Create new. This creates a key/secret with no permissions so it is recommended that you grant it permissions under Permissions. The secret for your key can be retrieved via the Display secret button.

> Do not share the secret part of your key as this is could allow someone to access the server as your application!

The secret cannot be reset at this time so if it is compromised, you will need to delete and generate a new key.

Permissions

Each key/secret pair has a set of permissions associated with it. This limits the endpoints you can call depending upon the permission. Permissions are broken down generally per game then a set of specific operations within that game such as console access.

Authenicating requests

When making calls to endpoints, you will need to pass in key/secret pair within the form data. Pass the key inside the `key` field and secret inside the `secret` field.

If the API credentials are invalid, you will receive a response with `status` set to `error` and `message` as `Invalid API credentials.` . You can see more detailed information in the `details` field.

Example error response:

```
{
 "status": "error",
 "message": "Invalid API credentials.",
 "details": "Key or secret are too short."
}
```

Revision #1
Created 13 March 2017 08:28:00
Updated 13 March 2017 08:48:02