

Endpoint Calls

Table of Contents

Events Endpoints.	2
Authentication Endpoints.....	3

Author: S. Schmidt

Version: draft – in process

Date: 05/05/2022

This document is a work in progress as the overall specification for the app is still being developed.

Version Changes:

Endpoint Calls

Events Endpoints.

Endpoint	JSON POST	JSON Received
/getevent GET	{ } Note: Requires header sent "Authorization": "Bearer 1234567890"	{ "_id": "626a068a40528be76454b522", "eventId": 1, "eventName": "<name>", "Description": "<description>", "Location": "<location details>", "dateTime": "<dd/mm/yy hh:mm:ss am/pm NZST>", }
/getevent?eventid=<id> GET	{ } Note: Requires header sent "Authorization": "Bearer 1234567890"	{ "_id": "626a068a40528be76454b522", "eventId": 1, "eventName": "<name>", "Description": "<description>", "Location": "<location details>", "dateTime": "<dd/mm/yy hh:mm:ss am/pm NZST>", }
/addevent POST	{ "eventName": "<name>", "Description": "<description>", "Location": "<location details>", "dateTime": "<dd/mm/yy hh:mm:ss am/pm NZST>", } Note: Requires header sent "Authorization": "Bearer 1234567890"	{ "eventId": 14, "acknowledged": true, "insertedId": "627360ce7a9f80295948529d" } Note: Returns new eventId which is used to reference the event in other calls.
/updevent?eventid=<id> POST	{ "eventId": <id>, "eventName": "<name>", "Description": "<description>", "Location": "<location details>", "dateTime": "<dd/mm/yy hh:mm:ss am/pm NZST>", } Note: Requires header sent "Authorization": "Bearer 1234567890"	{ "eventId": 1, "acknowledged": true, "matchedCount": 1, "modifiedCount": 1, "upsertedCount": 0 }
/delevent?eventid=<id> POST	{ } Note: Requires header sent "Authorization": "Bearer 1234567890"	{ "eventId": 14, "acknowledged": true, "deletedCount": 1 }

Note: If response is an error, a message detailing will accompany it.

Endpoint Calls

Authentication Endpoints.

Endpoint	JSON POST	JSON Received
/authenticate POST	{ "username": "admin", "password": "jumphigh" }	{ "authtoken": "whiterabbit:38fc406a686eebba7561", "expirytimestamp": 1651727982, "expirydatetime": "5/05/2022, 5:19:42 pm", "status": "Authenticated OK" }
/adduser POST	{ "authtoken": "whiterabbit:38fc406a686eebba7561", "username": "<desiredUsername>", "password": "<desiredPassword>" }	{ "authtoken": " whiterabbit:38fc406a686eebba7561", "expirytimestamp": 1651727447, "expirydatetime": "5/05/2022, 5:10:47 pm", "status": "Authenticated OK" }
/upduser POST	{ "authtoken": " whiterabbit:38fc406a686eebba7561", "username": "<desiredUsername>", "password": "<desiredPassword>", "Status": "A" or "D", "userLevel": "S" or "U" or "A", "staffID": "<ID of staff member>" } Notes: - all fields except authToken are optional. Status: "A" = Active "D" = Deactivated userLevel: "S" = Staff, "U" = User, "A" = Admin staffID: ID if associated with a staff member	{ "authtoken": " whiterabbit:38fc406a686eebba7561", "expirytimestamp": 1651727447, "expirydatetime": "5/05/2022, 5:10:47 pm", "status": "Authenticated OK" }
/getuser POST	{ "authtoken": " whiterabbit:38fc406a686eebba7561", "username": "<UsernameToRetrieve>" }	{ "_id": "6270e846550c8c89587cf667", "userid": 1, "username": "missy", "password": "BigDogg", "dateCreated": "3/05/2022 8:31:02 pm NZST", "status": "A", "userlevel": "S", "staffID": "", "lastLogin": "", "loginIP": "" }

Note: If response is an error, a message detailing will accompany it.