

# **Cannect Back-End Documentation**

Version 1.5.2

# 1 – Overview

## General Structure

The Cannect back-end is built with NodeJS, Express, and Mongoose. It is designed to interact with a MongoDB instance, specified with a hard-coded database URI in `server.js`, the main file. This project is separated into four primary folders, as follows.

- `models` – the folder containing any database schemas, registrations, and static methods.
- `routes` – the folder containing files that are responsible for registering endpoints on particular routes.
- `controllers` – the folder containing the files consisting of the logic for all endpoints.
- `middleware` – the folder containing any middleware used by the routers, primarily for authentication middleware at the moment.

## Database Objects

There are four primary categories of object present in this project, each of which has a model, route, and controller file, as follows.

- `Accounts` – User accounts.
- `Clinics` – Medicinal cannabis clinics.
- `Feedback` – Feedback for specific clinics.
- `Reviews` – Reviews given by a user for a particular clinic.

## 2 – Authentication

When sending any request to a protected endpoint, it is necessary to include an authorisation header with the following structure.

```
Bearer [Access Token]
```

If implemented successfully, the request will continue through to the endpoint, otherwise, one of the following responses will be generated.

- *No Authorisation Header* – An authorisation header was not provided.

```
401
{
  "code": 0
}
```

- *Malformed Header Provided* – The provided authorisation header was not of the correct form.

```
401
{
  "code": 1
}
```

- *Invalid Token Provided* – The provided JWT was invalid or expired.

```
401
{
  "code": 2
}
```

### Authorisation

If a request is sent to an endpoint requiring site administrator or clinic administrator permissions, and its access token is not linked to an account with those permissions, then the following response will be received.

```
403
```

## 3 – Accounts

### Account Registration

Request Element	Value		
Route	/api/account/register		
Method	POST		
Permissions	None		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	username	String	True
	password	String	True
	email	String	True
Successful Response	<pre>200 {   "access": [access token],   "refresh": [refresh token] }</pre>		
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Username Parameter	400 { "code": 0 }	
	Missing Password Parameter	400 { "code": 1 }	
	Duplicate Account Exists	400 { "code": 2 }	

### Logging In

Request Element	Value		
Route	/api/account/login		
Method	POST		
Permissions	None		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	username	String	True
	password	String	True

Successful Response	<pre>200 {   "access": [access token],   "refresh": [refresh token] }</pre>	
Errors	Error Cause	Error Response
	Missing Username Parameter	400 { "code": 0 }
	Missing Password Parameter	400 { "code": 1 }
	Account Does Not Exist	400 { "code": 2 }
	Password Incorrect	400 { "code": 3 }

## Refreshing Tokens

Request Element	Value		
Route	/api/account/refresh		
Method	POST		
Permissions	None		
JSON Body Parameters	Parameter Name	Parameter Type	Required
	refresh	String	True
Successful Response	<pre>200 {   "access": [access token] }</pre>		
Errors	Error Cause	Error Response	
	Missing Username Parameter	400 { "code": 0 }	
	Missing Password Parameter	400 { "code": 1 }	

## Account Deletion

Request Element	Value
Route	/api/account/delete
Method	DELETE
Permissions	Basic
Successful Response	200

## Updating an Account

Request Element	Value		
Route	/api/account/update		
Method	POST		
Permissions	Basic		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	new_username	String	False
	new_password	String	False
	old_password	String	True
Successful Response	200		
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Password Not Provided	400 { "code": 0 }	
	Incorrect Password	400 { "code": 1 }	

## Getting Account Information

Request Element	Value
Route	/api/account/get
Method	GET
Permissions	Basic
Successful Response	<pre>200 {   public_id: [public ID],   username: [username],   email: [email],   permission_level: [permission level] }</pre>

## Getting Other Account Information

Request Element	Value
Route	/api/account/getOther
Method	GET

Permissions	Basic		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	username	String	True (Either)
	account_id	String	
Successful Response	<pre>200 {   public_id: [public ID],   username: [username],   email: [email],   permission_level: [permission level] }</pre>		
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Account with Username DNE.	400 { "code": 0 }	
	Account with ID DNE.	400 { "code": 1 }	

## Account Deletion (Admin)

<b>Request Element</b>	<b>Value</b>		
Route	/api/account/deleteOther		
Method	DELETE		
Permissions	Site Administrator		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	account_id	String	True
Successful Response	200		
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Account Does Not Exist	400 { "code": 0 }	

## Updating an Account (Admin)

<b>Request Element</b>	<b>Value</b>		
Route	/api/account/updateOther		
Method	POST		
Permissions	Site Administrator		

JSON Body Parameters	Parameter Name	Parameter Type	Required
	new_username	String	False
	new_password	String	False
	account_id	String	True
Successful Response	200		
Errors	Error Cause	Error Response	
	Account Does Not Exist	400 { "code": 0 }	

## Get All Accounts (Admin)

Request Element	Value		
Route	/api/account/getAll		
Method	GET		
Permissions	Site Administrator		
Query Parameters	Parameter Name	Parameter Type	Required
	count	Integer	True
	offset	Integer	True
	sort_mode	Integer <ul style="list-style-type: none"> <li>• 0 – Alphabetically</li> <li>• 1 – Reverse Alphabetically</li> </ul>	False
Successful Response	<pre>200 {   [     {       "public_id": [account ID],       "username": [account username],       "email": [account email]     }   ], ... }</pre>		
Errors	Error Cause	Error Response	
	Missing Fields	400 { "code": 0 }	



## Elevating Account to Admin (Admin)

Request Element	Value		
Route	/api/account/elevateAdmin		
Method	POST		
Permissions	Site Administrator		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	account_id	String	True
Successful Response	200		
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Fields	400 { "code": 0 }	
	Account Does Not Exist	400 { "code": 1 }	

## Removing Admins (Admin)

Request Element	Value		
Route	/api/account/removeAdmin		
Method	POST		
Permissions	Site Administrator		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	account_id	String	True
Successful Response	200		
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Fields	400 { "code": 0 }	
	Account Does Not Exist	400 { "code": 1 }	

## 4 – Clinic Endpoints

### Clinic Creation

Request Element	Value		
Route	/api/clinic/create		
Method	POST		
Permissions	Site Administrator		
Successful Response	200		
JSON Body Parameters	Parameter Name	Parameter Type	Required
	name	String	True
	website	String	False
	email	String	False
	phone	String	False
	pharmacy_choice	Boolean	True
	referral_required	Boolean	True
	telehealth	Boolean	True
	concession_pricing	Boolean	True
	initial_consultation_fee	Number	True
	consultation_fee	Number	True
Errors	Error Cause	Error Response	
	Missing Required Parameter	400 { "code": 0 }	

### Clinic Deletion

Request Element	Value		
Route	/api/clinic/delete		
Method	DELETE		
Permissions	Site Administrator		
Query Parameters	Parameter Name	Parameter Type	Required
	id	String	True

Errors	Error Cause	Error Response
	Missing Clinic Parameter	400 { "code": 0 }
	Invalid Clinic Provided	400 { "code": 1 }

## Clinic Updating

Request Element	Value		
Route	/api/clinic/update		
Method	POST		
Permissions	Clinic Administrator		
Successful Response	200		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	clinic_id	String	True
	name	String	False
	website	String	False
	email	String	False
	phone	String	False
	telehealth	Boolean	False
	concession_pricing	Boolean	False
	pharmacy_choice	Boolean	False
	referral_required	Boolean	False
	initial_consultation_fee	Number	False
	consultation_fee	Number	False
Errors	Error Cause	Error Response	
	Missing Required Parameter	400 { "code": 0 }	
	Clinic Does Not Exist	400 { "code": 1 }	

## Getting Clinic Information

Request Element	Value		
Route	/api/clinic/get		
Method	GET		
Permissions	Basic		
Successful Response	<pre>200 {   "public_id": [clinic ID],   "name": [name],   "website": [website],   "email": [email],   "phone": [phone],   "pharmacy_choice": bool,   "referral_required": bool,   "telehealth": bool,   "concession_pricing": bool,   "initial_consultation_fee": number,   "consultation_fee": number,   "ratings": [     [# of 0-Star Reviews],     [# of 1-Star Reviews],     [# of 2-Star Reviews],     [# of 3-Star Reviews],     [# of 4-Star Reviews],     [# of 5-Star Reviews],    ],   "total_ratings": [# of ratings for clinic],   "average_rating": [average rating for clinic] }</pre>		
Query Parameters	Parameter Name	Parameter Type	Required
	id	String (Clinic ID)	True
Errors	Error Cause	Error Response	
	Missing ID Parameter	400 { "code": 0 }	
	Clinic Does Not Exist	400 { "code": 1 }	

## Clinic Searching

Request Element	Value		
Route	/api/clinic/search		
Method	GET		
Permissions	Basic		
Successful Response	<pre> 200 {   [     {       "public_id": [publicID],       "name": [name],       "website": [website],       "pharmacy_choice": [pharmacy choice],       "referral_required": [referral_required],       "concession_pricing": [concession pricing],       "initial_consultation_fee": [init. consultation fee],       "consultation_fee": [consultation fee],       "ratings" : [         [# of 0-Star Reviews],         [# of 1-Star Reviews],         [# of 2-Star Reviews],         [# of 3-Star Reviews],         [# of 4-Star Reviews],         [# of 5-Star Reviews],       ],       "total_ratings": [# of ratings for clinic],       "average_rating": [average rating for clinic]     }, ...   ] }</pre>		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	name	String (Clinic ID)	False
	pharmacy_choice	Boolean	False
	referral_required	Boolean	False
	telehealth	Boolean	False
	concession_pricing	Boolean	False
	init_consult_fee_min	Number	False
	init_consult_fee_max	Number	False

	consult_fee_min	Number	False
	consult_fee_max	Number	False

## Clinic Admin Elevation

Request Element	Value		
Route	/api/clinic/admin/elevate		
Method	POST		
Permissions	Site Administrator or Clinic Administrator		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	clinic_id	String (Clinic ID)	True
	account_id	String (Account ID)	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Invalid Account ID Provided	400 { "code": 0 }	
	Invalid Clinic ID Provided	400 { "code": 1 }	
	Account Already Administrator	400 { "code": 2 }	

## Clinic Admin Deletion

Request Element	Value		
Route	/api/clinic/admin/delete		
Method	DELETE		
Permissions	Site Administrator or Clinic Administrator		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	clinic_id	String	True
	admin_id	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Invalid Account Provided	400 { "code": 0 }	
	Invalid Clinic Provided	400 { "code": 1 }	
	Account Not Administrator	400 { "code": 2 }	

## Getting Clinic Reviews

Request Element	Value		
Route	/api/clinic/reviews		
Method	GET		
Permissions	Basic		
Successful Response	<pre> 200 {   [     {       "public_id": [review ID],       "text": [review text],       "rating": [numerical rating],       "date_submitted": [JS Date Obj],       "account_id": [public_id of reviewer]     },     ...   ] }</pre>		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	clinic_id	String (Clinic ID)	True
	count	Integer	True
	offset	Integer	True
	sort_mode	Integer <ul style="list-style-type: none"> <li>• 0 – Newest to Oldest</li> <li>• 1 – Oldest to Newest</li> <li>• 2 – Highest to Lowest</li> <li>• 3 – Lowest to Highest</li> </ul>	False
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Required Parameter.	400 { "code": 0 }	
	Invalid Clinic ID Provided	400 { "code": 1 }	

## 5 – Review Endpoints

### Review Creation

Request Element	Value		
Route	/api/review/create		
Method	POST		
Permissions	Basic		
Successful Response	200		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	clinic_id	String	True
	text	String	True
	rating	Number	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Required Parameter	400 { "code": 0 }	
	Clinic Does Not Exist	400 { "code": 1 }	
	Duplicate Review Exists	400 { "code": 2 }	

### Review Deletion

Request Element	Value		
Route	/api/review/delete		
Method	DELETE		
Permissions	Basic		
Successful Response	200		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	reviewID	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Review Does Not Exist	400 { "code": 0 }	
	Review Not Owned by Account	400 { "code": 1 }	



## Review Updating

Request Element	Value		
Route	/api/review/update		
Method	POST		
Permissions	Basic		
Successful Response	200		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	publicID	String (Review ID)	True
	newText	String	True (At least one)
	newRating	Integer (0-5, inc.)	
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Required Parameter	400 { "code": 0 }	
	Invalid Value for rating	400 { "code": 1 }	
	Review Does Not Exist	400 { "code": 2 }	
	Review Not Owned by Account	400 { "code": 3 }	

## Review Admin Deletion

Request Element	Value		
Route	/api/review/deleteOther		
Method	DELETE		
Permissions	Site Administrator		
Successful Response	200		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	reviewID	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Review Does Not Exist	400 { "code": 0 }	

## 6 – Feedback Endpoints

### Feedback Creation

Request Element	Value		
Route	/api/feedback/create		
Method	POST		
Permissions	Basic		
Successful Response	200		
JSON Body Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	text	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Missing Required Parameter	400 { "code": 0 }	

### Feedback Deletion

Request Element	Value		
Route	/api/feedback/delete		
Method	DELETE		
Permissions	Basic		
Successful Response	200		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	feedback_id	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Review Does Not Exist	400 { "code": 0 }	

### Getting Account Feedback

Request Element	Value
Route	/api/feedback/get
Method	GET

Permissions	Basic
Successful Response	<pre> 200 {   [     {       "public_id": [feedback ID],       "text": [feedback text],       "date_submitted": [date submitted]     }   ] }</pre>

## Delete Other Feedback (Admin)

Request Element	Value		
Route	/api/feedback/deleteOther		
Method	DELETE		
Permissions	Site Administrator		
Successful Response	<pre> 200</pre>		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	feedback_id	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Review Does Not Exist	<pre> 400 { "code": 0 }</pre>	

## Getting Other Feedback (Admin)

Request Element	Value		
Route	/api/feedback/getOther		
Method	GET		
Permissions	Site Administrator		
Successful Response	<pre> 200 {   [     {       "public_id": [feedback ID],       "text": [feedback text],       "date_submitted": [date submitted]     }   ] }</pre>		

	<pre>     ], ...   } </pre>		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	account_id	String	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Account Does Not Exist	400 { "code": 0 }	

## Getting All Feedback (Admin)

Request Element	Value		
Route	/api/feedback/getAll		
Method	GET		
Permissions	Site Administrator		
Successful Response	<pre> 200 {   [     {       "public_id": [feedback ID],       "text": [feedback text],       "date_submitted": [date submitted]     }   ], ... } </pre>		
Query Parameters	<u>Parameter Name</u>	<u>Parameter Type</u>	<u>Required</u>
	count	Integer	True
	offset	Integer	True
	sort_mode	Integer <ul style="list-style-type: none"> <li>• 0 – Newest to Oldest</li> <li>• 1 – Oldest to Newest</li> </ul>	True
Errors	<u>Error Cause</u>	<u>Error Response</u>	
	Review Does Not Exist	400 { "code": 0 }	