

For all Xs, we can create a pre-hook function that fetches the role of the requesting user. Then in the endpoints, have an object (Client, Role, Repairer, Role, ...) to give the function.

For the fly ones, grab the role from clickstaff table in db.

Method	Path	Description	Client	Repairer	Event manager	Admin	Comments	Possible Implementation	Role	Description	Possible Implementation
GET	/event	Get events	0	0	0	0	Hide detailed information like assignees For the events carousel which is public		Client	Submit repair requests Can view their own repair requests Get assigned to events Can view events they're assigned to	"Created by me" filter (realistically == user)
POST	/event	Create events	X	X	0 [1]	0	Event and org manager can only create an event for orgs they're in	Org filter	Repairer	Can view their own repair requests Can view events they're assigned to Get repair requests if they're assigned	"Assigned" filter
GET	/event[id]	Get event (detailed info)	X	X	0	0	Event and org manager can only get for orgs they're in	Repairer assigned and unassigned filter Event manager is a manager for event Organisation manager, organisation filter	Event manager	Create events on behalf of org manager Assign requests to events (?) and items	"My organisations" filter
GET	/event[id]/repair-request	Get repair requests	X	0 [3]	0 [4]	0	Repairer can only see requests they're assigned to Event manager can see requests if they're assigned to Organisation manager can see if the event is part of their organisations		Admin	Can do everything	Add a pre-hook for requests to always allow admin
GET	/event[id]/options	Get event options	0	0	0	0	Gets only id and name for events				
GET	/repair-request	Get OWN repair requests	0	0	0	0	Doesn't exist				
POST	/repair-request	Create repair request	0	0	0	0	Need to rate limit				
PATCH	/repair-request[id]	Update repair request	0 [8]	0	0	0	Client can only update their own request Client can only get for their own request Consider changing the path to /repair-request[id]/images?				
GET	/repair-request/images	Get a single repair request's images	0 [7]	0	0	0					
GET	/user	Get users	X	0	0	0	Limited to organisation unless super admin				
GET	/user[id]	Get user	X	0	0	0	Limited to organisation unless super admin				
PATCH	/user[id]/role	Update a user's role	X	X	X	0 [8]	Organisation manager can only edit role for users that are in their org	reqUserOrgs.some(ownOrgs)			
GET	/brand	Get brands	0	0	0	0	Delete from schema in favour of adding field				
GET	/item-type	Get item types	0	0	0	0					
POST	/upload-image	Upload image and get url	0	0	0	0	Need to rate limit, lock down more by requiring a repair request id and setting max images on repair request Would need to be moved to /repair-request[id]/upload-image 1. Create repair request 2. With response, upload images				
GET	/organisation	Get organisations	X	X	X	0	Doesn't exist				
POST	/organisation	Create organisation	X	X	X	X	Doesn't exist				
PATCH	/organisation	Update organisation	X	X	X	X	Doesn't exist				
PUT	/organisation/@/user	Add user to org	X	X	X	0 [9]	Doesn't exist. Organisation manager can only add users to organisations they're a part of	Org guard			
DELETE	/organisation/@/user	Remove user from org	X	X	X	0 [10]	Doesn't exist. Organisation manager can only add users to organisations they're a part of	Org guard			

[1] Can only create an event for orgs they're in  
-dct

[2] Can only create an event for orgs they're in  
-dct

[3] Can only see unassigned repair requests and repair request assigned to them  
-dct

[4] If they are a manager of the event  
-dct

[5] Only if the event belongs to the manager's organisation  
-dct

[6] Can only update their own repair request  
-dct

[7] If it's their own request  
-dct

[8] Only users that are in the org  
-dct

[9] If they're part of the org  
-dct

[10] If they're part of the org  
-dct